JOURNAL OF ALGEBRA 166, 481–505 (1994)

Maximal Abelian Normal Subgroups of Galois Pro-2-Groups

ANTONIO JOSÉ ENGLER*

Departamento de Matemática, IMECC, UNICAMP, Caixa Postal 6065, 13.081, Campinas, SP, Brasil

AND

JOÃO BOSCO NOGUEIRA†

Departamento de Matemática, CCEN, Universidade Federal da Paraiba, 58.059, João Pessoa, PB, Brasil

Communicated by Alexander Lubotzky

Received June 26, 1991

1. INTRODUCTION

The aim of this paper is to show that the Galois group of the quadratic closure of any field K contains a largest abelian normal subgroup $\mathfrak{U}$. (That is, $\mathfrak{U}$ is an abelian normal subgroup of K that contains any other such a subgroup.)

Throughout this paper we denote by K a field of characteristic not 2, by $K(2)$ its quadratic closure, by K^* the multiplicative group of K, and by $q(K)$ the subgroup of non-zero squares. The fields of characteristic 2 are excluded because of Remark 3.6(c), since in this case $\mathfrak{U}$ has to be trivial.

This work is based on valuation theoretical methods. In Section 2 we present the results on valuation rings that we shall need. Theorems 2.10 and 2.14 are the most important tools to prove the main theorem of this paper.

In Section 3, we first examine the particular case where $\mathfrak{U} \cong \mathbb{Z}_2$, the group of the 2-adic integers. In Section 4 we consider the general case and then we state our main result. Specifically, we will prove that for every field K the Galois group $G(K) = \mathrm{Gal}(K(2); K)$ contains the largest normal abelian subgroup. This result generalizes [3, Chapter III, Theorem 1,

* Supported in part by the CNPq.

† Supported in part by the CAPES via PICD.

0021-8693/94 $6.00

p. 86] and [19, Theorem 4.1], where the theorem was proved for C-fields. We also obtain a generalization of the results of Ware, see [21, Theorems B and C] and [22, Corollary 2 of Theorem 1], where he characterizes the normal abelian subgroups of $G(K)$ and gives bounds on the rank of arbitrary abelian subgroups of $G(K)$.

All groups we shall consider are pro-2-groups and all subgroups are assumed to be closed subgroups. We shall denote by $\langle S \rangle$ the closed subgroup generated by a subset S, by $r(G)$ the rank of a pro-2-group G and by $(G : H)$ the index of H in G for any subgroup H of G.

2. Valuations

In this section we present some facts on the 2-henselian valuations rings, which have been derived from the henselian valuation rings (see [9, 10]). These results will be used later on in this paper.

Let us introduce some notations. For every valuation ring A we denote by A^*, m_A, $\mathscr{K}_A$, and Γ_A the group of units of A, the maximal ideal, the residue class field and the value group of A, respectively. For every field K let $c(K)$ be its characteristic. If $c(\mathscr{K}_A) \neq 2$ the valuation ring A is called non-dyadic. For all other notations and terminology we shall follow [7].

2.1. Definition [3, 5]. A valuation ring A of a field K will be called 2-henselian if and only if A admits at most one extension to $K(2)$. This unique extension will be denoted by $\tilde{A}$.

Observe that if K is quadratic separably closed then every valuation ring A of K is 2-henselian.

Another characterization of 2-henselian valuation rings, which is most useful, is given by the following proposition due to Bröcker.

2.2. Proposition (Hensel's Lemma [5, 1.2]). *Let A be a valuation ring of a field K. Then the following conditions are equivalent*:

(a) *A is 2-henselian.*

(b) *For any polynomial $f(X) \in A[X]$, of degree two, such that $\bar{f}(X)$ has two distinct roots $\bar{a}, \bar{b} \in \mathscr{K}_A$, there are roots $x, y \in A$ of $f(X)$, such that $\bar{x} = \bar{a}$ and $\bar{y} = \bar{b}$.*

Proof. Use [5, Lemma 1.2] and [6, Satz 1]. ∎

2.3. Corollary [5, 1.4]. *Any field K which has two independent 2-henselian valuation rings is quadratic separably closed.* ∎

The following proposition can be considered as a partial generalization of the above corollary.

2.4. PROPOSITION [9, Proposition]. *Let A be a valuation ring of K which is incomparable to some 2-henselian valuation ring A' of K. Then $\mathcal{K}_A$ is quadratically closed.* ▮

It follows from this proposition that every valuation ring A of a quadratic separably closed field K has $\mathcal{K}_A$ quadratically closed.

Let $\mathcal{H}(K)$ be the set of all 2-henselian valuation rings of K. In order to describe completely $\mathcal{H}(K)$ we split $\mathcal{H}(K)=\mathcal{H}_1(K)\cup\mathcal{H}_2(K)$, as in [9], where $\mathcal{H}_1(K)=\{A\in\mathcal{H}(K)\mid\mathcal{K}_A$ is not quadratic separably closed$\}$ and $\mathcal{H}_2(K)=\{A\in\mathcal{H}(K)\mid\mathcal{K}_A$ is quadratic separably closed$\}$. If we consider these sets as subsets of the set of all valuation rings of K they have the following properties:

2.5. PROPOSITION [9, Corollary 1]. (a) *Let $A\in\mathcal{H}(K)$ and let C be a valuation ring of K. If $A\subseteq C$, then $C\in\mathcal{H}(K)$.*

(b) *$\mathcal{H}_1(K)$ is totally ordered by inclusion and if A and C are valuation rings of K such that $A\in\mathcal{H}_1(K)$ and $A\subseteq C$, then $C\in\mathcal{H}_1(K)$.*

(c) *Let A and C be valuation rings of K. If $A\in\mathcal{H}_2(K)$ and $C\subseteq A$, then $C\in\mathcal{H}_2(K)$. If A, $C\in\mathcal{H}_2(K)$, then their product D is also an element of $\mathcal{H}_2(K)$ and so $\mathcal{H}_2(K)$ is a directed set. (Recall that the product D, of two valuation rings A and C, is the smallest subring of K containing both A and C.)*

(d) *For all $A_1\in\mathcal{H}_1(K)$ and $A_2\in\mathcal{H}_2(K)$ we have that $A_2\subset A_1$.* ▮

As in [9] we get from Proposition 2.5(b) that $A_{(1)}=\bigcap A$, for all $A\in\mathcal{H}_1(K)$, is a valuation ring of K. Now, if $\mathcal{H}_2(K)$ is non-empty, let us take $A_{(2)}=\bigcup A$, for all $A\in\mathcal{H}_2(K)$. By Proposition 2.5(c), $A_{(2)}$ is also a valuation ring of K. It is an easy consequence of the statements above and of Theorem 2.15 below that they satisfy:

2.6. PROPOSITION [9, Corollary 2]. (a) *We have $A_{(1)}\in\mathcal{H}(K)$ and $A_{(1)}\in\mathcal{H}_1(K)$ if and only if $\mathcal{H}_1(K)$ has a smallest element. In particular, this is the case whenever $\mathcal{H}_2(K)$ is empty.*

(b) *If $\mathcal{H}_2(K)$ is non-empty, then $A_{(2)}$ is the largest element of $\mathcal{H}_2(K)$. We have $A_{(2)}\subseteq A_{(1)}$ and there is no ring strictly contained between $A_{(2)}$ and $A_{(1)}$. Moreover, $A_{(2)}=A_{(1)}$ if and only if $A_{(1)}\notin\mathcal{H}_1(K)$. Let $A\in\mathcal{H}_2(K)-\{A_{(2)}\}$, then $\mathcal{K}_A$ is quadratically closed and Γ_A has a non-trivial 2-divisible convex subgroup Δ such that $\Gamma_{(2)}=\Gamma_A/\Delta$, where $\Gamma_{(2)}$ is the value group of $A_{(2)}$.*

Proof. The proof of (a) and the first part of (b) follows as in [9, Corollary 2]. In order to prove the last statement of (b), let $\mathcal{K}_{(2)}$ be the residue field of $A_{(2)}$ and for every $A \in \mathscr{H}_2 - \{A_{(2)}\}$ let $\bar{A}$ be its image in $\mathscr{K}_{(2)}$. Since $\mathscr{K}_{(2)}$ is quadratic separably closed, $\bar{A}$ has residue field quadratically closed as it was observed soon after Proposition 2.4. Since the residue fields of $\bar{A}$ and $\mathscr{K}_A$ are isomorphic it follows that $\mathscr{K}_A$ is quadratically closed.

On the other hand if Δ is the convex subgroup of Γ_A such that $\Gamma_{(2)} = \Gamma_A/\Delta$, then Δ and $\Gamma_{\bar{A}}$ (the value group of $\bar{A}$) are isomorphic. Thus we just have to show that $\Gamma_{\bar{A}}$ is a 2-divisible group to finish the proof. Suppose this is not the case and let Γ be a totally ordered group such that $\Gamma_{\bar{A}} \subset \Gamma$ and $(\Gamma : \Gamma_{\bar{A}}) = 2$. By [7, 27.1] there exists a separable extension $\mathscr{L}$ of $\mathscr{K}_{(2)}$ such that $[\mathscr{L} : \mathscr{K}_{(2)}] = (\Gamma : \Gamma_{\bar{A}}) = 2$. But this contradicts the fact that $\mathscr{K}_{(2)}$ is quadratic separably closed. ∎

We now shall take a look on the subset of $\mathscr{H}(K)$ consisting of all valuation rings which are $q(K)$-compatible according to the following definition:

2.7. Definition [1]. A valuation ring A of K is $q(K)$-compatible if $1 + m_A \subseteq q(K)$.

2.8. *Remark.* If $c(K) \neq 2$, a $q(K)$-compatible valuation ring is 2-henselian by [20, Lemma 4.3] or [6, Satz 2]. The converse holds if A is non-dyadic by Proposition 2.2 or [6, Satz 2].

As it was shown in [20] and [1] $q(K)$-compatible valuation rings are raised by rigid elements. Following Ware [21] an element a in K is called *rigid* if $a \notin q(K) \cup -q(K)$ and $x^2 + ay^2 \in q(K) \cup aq(K)$ for all $x, y \in K$. The element a is called *double rigid* if a and $-a$ are rigid.

The set of all elements in K^* which are not double rigid (the set of basic elements) is denoted by $B(K)$ and it is a subgroup of K^*, by [20, Proposition 2.4].

2.9. Definition [1]. A field K is called *exceptional* if $B(K) = \pm q(K)$ and either $-1 \in q(K)$ or $q(K)$ is additively closed.

We now present two technical results which are crucial to our arguments. The first one is the next theorem. The other one is Theorem 2.14.

As in [7, Sect. 19], we shall denote by $G^T(D; K)$ the inertia group of D over K for every valuation ring D of $K(2)$ and by $K^T(D; K)$ the fixed field of $G^T(D; K)$.

2.10. Theorem [1]. *Let K be a field for which there exists $A \in \mathscr{H}(K)$ such that $c(\mathscr{K}_A) \neq 2$ and $\Gamma_A \neq 2\Gamma_A$. Then there exists a unique $q(K)$-compatible valuation ring $O(K)$ of K such that:*

(a) *$B(K) \subseteq O(K)^* q(K)$ and $(O(K)^* q(K) : B(K)) \leqslant 2$. Moreover, if K is not exceptional, then $O(K)^* q(K) = B(K)$.*

(b) *$B(K) \neq K^*$ and $(\mathscr{K}^*_{\tilde{O}(K)} : B(\mathscr{K}_{O(K)})) \leqslant 2$. Furthermore, if K is not exceptional, then $B(\mathscr{K}_{O(K)}) = \mathscr{K}^*_{\tilde{O}(K)}$.*

(c) *$O(K)$ is non-dyadic. In particular $G^T(\tilde{O}(K); K)$ is a normal abelian subgroup of $G(K)$ such that $r(G^T(\tilde{O}(K); K)) = r(K^* : O(K)^* q(K))$ (see Definition 2.1 for the meaning of $\tilde{O}(K)$). Furthermore, let Λ be a set of indices of cardinality $r(K^*/O(K)^* q(K))$. Then every subset $\{a_\lambda \mid \lambda \in \Lambda\}$ of K^* that is an $\mathbb{F}_2$-basis of K^* modulo $O(K)^* q(K)$ is also an $\mathbb{F}_2$-basis of $K^T(\tilde{O}(K); K)^*$ modulo $q(K^T(\tilde{O}(K); K))$.*

(d) *$\Gamma_{O(K)}$ has no non-trivial 2-divisible convex subgroup. In particular $\Gamma_{O(K)}$ is not 2-divisible.*

(e) *For every $A \in \mathscr{H}(K)$ such that $c(\mathscr{K}_A) \neq 2$ and Γ_A contains no non-trivial 2-divisible convex subgroup $O(K) \subseteq A$.*

Proof. First we shall prove that there exists a proper, $q(K)$-compatible, valuation ring C of K such that Γ_C contains no non-trivial 2-divisible convex subgroups. (Observe that a "T-coarse valuation ring" C ([1, Definition 3.3]) means, in the present case, that Γ_C contains no non-trivial 2-divisible convex subgroup.) Let Δ be the maximal convex subgroup of $2\Gamma_A$ and C be the valuation ring containing A, which corresponds to Γ_A/Δ (as stated by Theorem 7.4 of [7]). Hence Γ_C contains no non-trivial 2-divisible convex subgroups by construction. Since $A \subseteq C$ and A is $q(K)$-compatible, so is C.
Now, by [1, Theorem 3.8] there exists a unique smallest valuation ring $O(K)$ of K for which (d) and (e) hold.

Proof of (a). Theorem 3.9 of [1] implies that $B(K) \subseteq O(K)^* q(K)$, $(O(K)^* q(K) : B(K)) \leqslant 2$ and $B(K) = O(K)^* q(K)$ if K is not exceptional.

Proof of (b). By (a) and (d) $B(K) \neq K^*$. The other statements are consequence of (a), and [1, Proposition 1.9].

Proof of (c). Lemma 4.4 of [1] yields that $O(K)$ is non-dyadic. Hence the ramification group of $\tilde{O}(K)$ over K is trivial by [7, Corollary 20.18]. Thus $G^T(\tilde{O}(K); K)$ is an abelian subgroup of $G(K)$ by [7, Theorem 20.12]. Now, we simplify the notations by writing $H = O(K)^* q(K)$ and $K^T = K^T(\tilde{O}(K); K)$. We shall show that the map $\varphi\colon K^*/H \to (K^T)^*/q(K^T)$, given by $\varphi(xH) = xq(K^T)$ for every $x \in K^*$, is an isomorphism. This ends the proof since $r(G^T(\tilde{O}(K); K)) = r((K^T)^*/q(K^T))$.

Recall first that the value group of $\tilde{O}(K) \cap K^T$ and $O(K)$ are equal. Take $x \in K^*$ such that $x = y^2$ for some $y \in K^T$. The above observation yields $x \in O(K)^* q(K) = H$. Therefore φ is an injection. Take now $y \in (K^T)^*$. The same observation implies that there exists $x \in K^*$ such that yx^{-1} is a unit of $\tilde{O}(K) \cap K^T$. Since the residue class field of $\tilde{O}(K) \cap K^T$ is quadratically closed there exists another unit z of $\tilde{O}(K) \cap K^T$ such that $yx^{-1} = z^2$. Hence φ is also a surjection and the proof of (c) is complete. ▮

In the next proposition we get conditions for the existence of a valuation ring A as in the above theorem.

2.11. PROPOSITION. *For any field K with $(K^* : B(K)) > 2$ or such that $(K^* : B(K)) = 2$, but K is not exceptional, there exists a 2-henselian non-dyadic valuation ring A such that Γ_A is not 2-divisible.*

Proof. We need to use Theorem 2.16 of [1] (take $T = q(K)$ and $H = B(K)$). This theorem implies that there exist a subgroup $\hat{H}$ of K^* and a valuation ring A of K, for which the following statements are true:

(1) $(\hat{H} : B(K)) \leqslant 2$ and $\hat{H} = B(K)$ unless K is an exceptional field,

(2) A is $q(K)$-compatible and $A^* q(K) \subseteq \hat{H}$.

By the assumptions we have made on $B(K)$ it follows that $\hat{H} \neq K^*$ and so A is a proper valuation ring of K. Let v be the valuation corresponding to A and Γ_A. Since $A^* q(K) \subseteq \hat{H}$, $2\Gamma_A = v(A^* q(K)) \subseteq v(\hat{H})$. By [1, Lemma 3.1] $v(\hat{H})$ contains no non-trivial convex subgroups of Γ_A. Hence Γ_A does not have a non-trivial 2-divisible convex subgroup. Now, following Lemma 4.4 of [1], we shall prove that A is non-dyadic. Suppose that $c(\mathscr{K}_A) = 2$. Then $c(K) = 0$, since $c(K) \neq 2$. Let $\Delta \neq \{0\}$ be the convex subgroup of Γ_A generated by $v(2)$. Since Δ is not contained in $2\Gamma_A$ we claim that there exists $\delta \in \Delta$ satisfying $0 < \delta < v(4)$. Choose $\lambda > 0$, $\lambda \in \Delta - 2\Gamma_A$ and let $n \geqslant 0$ satisfy $2nv(2) < \lambda < (2n+2)\, v(2)$. Then $\delta = \lambda - 2nv(2)$ is as required. Let $e \in K^*$ be such that $v(e) = \delta$. Then $e \in m_A$, $1 + e \in 1 + m_A \subseteq q(K)$ and so $D(\langle 1, -(1+e) \rangle) = \{x^2 - (1+e)\, y^2 \neq 0 \mid x, y \in K\} = K^*$. But this cannot be true since [1, Lemma 4.3] yields $D(\langle 1, -(1+e) \rangle) \subseteq q(K) \cup eq(K)$. This contradiction shows that $\Delta = \{0\}$. ▮

Next, we shall state two propositions that will be used in Section 4.

2.12. PROPOSITION. *Using the notation introduced before Proposition 2.6 and assuming the existence of $O(K)$, we have:*

(a) *If $O(K) \in \mathscr{H}_2(K)$, then $O(K) = A_{(2)}$, $B(K) = q(K)$, and $G(K) = G^T(\tilde{O}(K); K)$ is an abelian group.*

(b) *Let $A \in \mathscr{H}(K)$ be non-dyadic, then A is comparable to $O(K)$. If $A \subseteq O(K)$, then $G^T(\tilde{A}; K) = G^T(\tilde{O}(K); K)$.*

Proof. (a) Since $c(\mathscr{K}_{O(K)}) \neq 2$ by 2.10(c), if $O(K) \in \mathscr{H}_2(K)$, then $O(K)^* \subseteq q(K)$. Hence $B(K) = q(K)$ by 2.10(a). On the other hand, we have

$O(K) \subseteq A_{(2)}$ and by Theorem 2.10(d), $\Gamma_{O(K)}$ has no non-trivial 2-divisible convex subgroup. Thus Proposition 2.6(b) implies that $O(K) = A_{(2)}$ as required.

(b) If A and $O(K)$ are incomparable, Proposition 2.5 implies that A, $O(K) \in \mathscr{H}_2(K)$. By (a), $O(K) = A_{(2)}$, and so $A \subseteq O(K)$, contradiction.

Assume now that $A \subseteq O(K)$. Theorem 3.8 of [1] implies that Γ_A has a non-trivial 2-divisible convex subgroup Δ such that $\Gamma_{O(K)} = \Gamma_A/\Delta$. Let C be the image of $\tilde{A}$ in $\mathscr{K}_{O(K)}(2)$ and $\bar{A} = C \cap \mathscr{K}_{O(K)}$. Then $\bar{A}$ is the image of A in $\mathscr{K}_{O(K)}$ and has value group isomorphic to Δ, which is 2-divisible. Hence $C \cap K^T(C; \mathscr{K}_{O(K)})$ has also a 2-divisible value group. Thus [7, Theorem 19.12] and $c(\mathscr{K}_A) \neq 2$, imply that $K^T(C; \mathscr{K}_{O(K)}) = \mathscr{K}_{O(K)}(2)$. Hence $K^T(\tilde{A}; K) = K^T(\tilde{O}(K); K)$, by [7, 19.13]. ∎

2.13. Proposition. *Let $L \mid K$ be an extension of fields, $L \subseteq K(2)$, and A a valuation ring of L such that there is no non-trivial 2-divisible convex subgroup of Γ_A. Then $A \cap K$ has the same property.*

Proof. Let $C = A \cap K$. Since Γ_A/Γ_C is a 2-torsion group, by [7, 13.11], every 2-divisible convex subgroup of Γ_C is also a convex subgroup of Γ_A. ∎

2.14. Theorem. *Let K be a field, and let C, C' be incomparable valuations rings of $K(2)$. If D is their product the following equalities hold:*

$$G^Z(C; K) \cap G^Z(C'; K) = G^T(C; K) \cap G^T(C'; K) = G^T(D; K).$$

Proof. The proof follows as in Theorem 2.2 of [10] using Corollary 2.3. ∎

As a consequence of this Theorem we get the following "going down" result for 2-henselian valuation rings.

2.15. Theorem. *Let $N \mid K$ be normal and $N \subset K(2)$, $N \neq K(2)$. Assume that there is C, a proper 2-henselian valuation ring of N, such that $C \cap K$ is not 2-henselian. Then there exists D, a proper valuation ring of N, containing C, such that $D \cap K$ is 2-henselian and $K^T(\tilde{D}; K) \subseteq N$.*

Furthermore, D can be chosen to be the smallest in the sense that $D \subseteq D'$ for every valuation ring D' of N such that $C \subseteq D'$ and $D' \cap K$ is 2-henselian.

Proof. It follows from the Theorem above as in [10, Theorem 3.3]. ∎

The following statement will be used in Section 4.

2.16. Corollary. *Let K be a field for which the following conditions hold:*

(1) *There exists a normal extension E of K, $K \subseteq E \subset K(2)$ $(E \neq K(2))$.*

(2) *There exists an extension F of K, $F \subseteq E$, such that F has a non-dyadic, 2-henselian valuation ring C with $\Gamma_C \neq 2\Gamma_C$.*

Then K fulfills the hypothesis of Theorem 2.10.

Proof. Observe that $\tilde{C} \cap E$ is a proper, non-dyadic, 2-henselian valuation ring of E. Theorem 2.15 therefore yields a proper 2-henselian valuation ring D of E containing $\tilde{C} \cap E$ such that $D \cap K$ is 2-henselian and either $D = \tilde{C} \cap E$ or $K^T(\tilde{D}; K) \subseteq E$. Since $\tilde{C} \cap E \subseteq D$, D is also non-dyadic. If $D = \tilde{C} \cap E$, the value group of $D \cap K = C \cap K$ is not 2-divisible since $\Gamma_C \neq 2\Gamma_C$. Thus $A = D \cap K$ is a non-dyadic, 2-henselian valuation ring of K such that $2\Gamma_A \neq \Gamma_A$. If $D \neq \tilde{C} \cap E$, we assert that the value group of $D \cap K$ is again not 2-divisible. Indeed, [7, Corollary 20.14] implies that $G^V(\tilde{D}; K)$ is a trivial subgroup since D is a non-dyadic valuation ring. By [7, Theorem 20.12], if $D \cap K$ has a 2-divisible valued group, $K^T(\tilde{D}; K) = K(2)$ which is contrary to $K^T(\tilde{D}; K) \subseteq E \neq K(2)$. Thus, as before, $A = D \cap K$ is a valuation ring of K with the required properties. ∎

3. The Particular Case $\mathfrak{U} = \mathbb{Z}_2$

For every field K and every subgroup H of $G(K)$ let $C(H) = \{g \in G \mid gh = hg\ \forall h \in H\}$ be the centralizer of H. Observe that $C(\langle \sigma \rangle) = \langle \sigma \rangle$ for every involution σ of $G(K)$, by [3, Chapter II, Corollary of Theorem 4, p. 78].

3.1. Proposition. *Let G be a pro-2-group such that:*

(i) *If $g \in G$, $g \neq 1$, has finite order, then g is an involution.*

(ii) *For every involution $\sigma \in G$, $C(\langle \sigma \rangle) = \langle \sigma \rangle$.*

(iii) *There exists a normal subgroup $U \cong \mathbb{Z}_2$.*

Then, we have either

(a) *there exists a normal subgroup U' of G such that $U \subseteq U'$, $U' \cong \mathbb{Z}_2$ and $C(U') = U'$; or*

(b) *there exists $g \in C(U)$ and $g \notin U$ such that $\langle g \rangle \cap U = \{1\}$. In this case $\langle g \rangle \times U \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is a subgroup of G.*

Proof. Let $\mathcal{G} = \{H \mid H \cong \mathbb{Z}_2$ is a normal subgroup of G containing $U\}$. Using Zorn's Lemma we get that $\mathcal{G}$ has a maximal element U'.

We show that if $C(U') \neq U'$, then (b) holds. Suppose that for every $g \in C(U')$, $g \notin U'$ we have that $\langle g \rangle \cap U' \neq \{1\}$. For every such g there is a natural number n such that $g^n \in U'$. Hence $C(U')/U'$ is a 2-torsion group. Let us define $o(g) =$ the order of the element $gU' \in C(U')/U'$, for every $g \in C(U')$.

We *claim* that if $o(g)=2^s$, where $s>0$, then $\langle g^{2^s}\rangle = U'$. Let $2^r = (U' : \langle g^{2^s}\rangle)$, where $r \geqslant 0$. Thus $\langle g^{2^s}\rangle = (U')^{2^r}$. Hence there is $h\in U'$ such that $g^{2^s}=h^{2^r}$. It is sufficient to show that $r=0$. Suppose first that $r\geqslant s$. Since g and h commute we have that $(h^{2^{r-s}}g^{-1})^{2^s}=1$. Since $g\in C(\langle h^{2^{r-s}}g^{-1}\rangle)$, condition (i) says that $h^{2^{r-s}}g^{-1}$ is not an involution. Thus $g=h^{2^{r-s}}\in U'$, contradicting $g\notin U'$. If $s>r$, we get in the same way $g^{2^{s-r}}h^{-1}=1$. Thus $g^{2^{s-r}}\in U'$. The minimality of 2^s forces $r=0$ and the *claim* is proved.

Since $C(U')/U'$ is a torsion pro-2-group it has elements of order two. Let us take $g\in C(U')$ such that $o(g)=2$. If for every $g'\in C(U')$ such that $o(g')=2$ we have that $\langle g\rangle = \langle g'\rangle$, then $\langle g\rangle$ is a normal subgroup of G. Since $U'=\langle g^2\rangle \subset \langle g\rangle$, this contradicts the maximality of U'. Thus, there are $g_1, g_2\in C(U')$ such that $o(g_1)=2=o(g_2)$ and $\langle g_1\rangle \neq \langle g_2\rangle$. Let $h=g_1g_2\in C(U')$. Since $h^{o(h)}\in U'$ and $g_1\in C(U')$ we have that $g_1(h^{o(h)})g_1^{-1}=h^{o(h)}$. On the other hand, since $g_1^2\in U'$ and $g_2g_1^{-1}\in C(U')$ it follows that $g_1hg_1^{-1}=g_1(g_1g_2)g_1^{-1}=g_1^2(g_2g_1^{-1})=(g_2g_1^{-1})g_1^2=g_2g_1$ and so $g_1(h^{o(h)})g_1^{-1}=g_1(g_1g_2)^{o(h)}g_1^{-1}=(g_2g_1)^{o(h)}$. Hence $(g_1g_2)^{o(h)}=(g_2g_1)^{o(h)}$.

Now, observe that $(g_1g_2)(g_2g_1)=g_1g_2^2g_1=g_1^2g_2^2$ and $(g_2g_1)(g_1g_2)=g_2g_1^2g_2=g_1^2g_2^2$. Therefore, g_1g_2 commutes with g_2g_1 and so $[(g_1g_2)(g_2g_1)^{-1}]^{o(h)}=1$. Furthermore, $U'\subseteq C(\langle (g_1g_2)(g_2g_1)^{-1}\rangle)$ shows that $(g_1g_2)(g_2g_1)^{-1}$ is not an involution. Hence $(g_1g_2)(g_2g_1)^{-1}=1$ and g_1 commutes with g_2. Since $\langle g_1^2\rangle = U' = \langle g_2^2\rangle$ and $U'=(U')^2\cup g_1^2(U')^2$ there exists $u\in U'$ such that $g_2^2=g_1^2u^2$. Hence $(g_2^{-1}g_1u)^2=1$, which already implies $g_2=g_1u$. Thus $\langle g_2\rangle \subseteq \langle g_1\rangle$. If we change the roles of g_1 and g_2 in the last lines we get $\langle g_1\rangle\subseteq\langle g_2\rangle$. Then $\langle g_1\rangle=\langle g_2\rangle$ contradicting the choice of g_1 and g_2. This contradiction shows that there is $g\in C(U')\subseteq C(U)$ such that $\langle g\rangle\cap U\subseteq\langle g\rangle\cap U'=\{1\}$. Hence (b) is true. ∎

In the next theorem we shall give a complete description of the fields K such that $G(K)$ satisfies the condition (a) of the last Proposition. We shall need the following two lemmata.

3.2. LEMMA. *Let $G=\langle\tau\rangle\rtimes\langle\sigma\rangle\cong\mathbb{Z}_2\rtimes\mathbb{Z}_2$ (G is a semidirect product of $\mathbb{Z}_2$ by $\mathbb{Z}_2$) be a non-abelian group where $C(\langle\tau\rangle)=\langle\tau\rangle$. Then every abelian normal subgroup T of G is contained in $\langle\tau\rangle$. Furthermore, if $G/T\cong\mathbb{Z}_2$, then $T=\langle\tau\rangle$.*

Proof. Let $\sigma\tau\sigma^{-1}=\tau^\lambda$, where λ is a unit of the ring $\mathbb{Z}_2$. Since G is not commutative, $\lambda\neq 1$. If $\lambda=-1$, then $\sigma^2\tau\sigma^{-2}=\tau$ and $\sigma^2\in C(\langle\tau\rangle)$, contradicting $C(\langle\tau\rangle)=\langle\tau\rangle$. Thus $\lambda\in\pm 1+4\mathbb{Z}_2$ by [16, Proposition 8, p. 32]. Replacing τ by τ^{-1} if necessary, we may assume without loss of generality that $\lambda\in 1+4\mathbb{Z}_2$. Let $\lambda\in 1+2^n\mathbb{Z}_2$ and $\lambda\notin 1+2^{n+1}\mathbb{Z}_2$, for some $n\geqslant 2$.

We *claim* that for every $\delta,\gamma\in\mathbb{Z}_2$, $\delta,\gamma\neq 0$, $\sigma^\delta\tau^\gamma\sigma^{-\delta}=\tau^\gamma$ cannot occur. First we observe that $\sigma^\delta\tau^\gamma\sigma^{-\delta}=(\sigma^\delta\tau\sigma^{-\delta})^\gamma=\tau^{\gamma\lambda^\delta}$. Next, from the proof of

Proposition 8 of [16] we get that every $\omega \in (1+4\mathbb{Z}_2) - (1+8\mathbb{Z}_2)$ is a generator of $1+4\mathbb{Z}_2$ as a $\mathbb{Z}_2$-module; that is, $\omega^{\mathbb{Z}_2} = 1+4\mathbb{Z}_2$. Thence $\lambda \in (1+2^n\mathbb{Z}_2) - (1+2^{n+1}\mathbb{Z}_2)$ is also a generator of $1+2^n\mathbb{Z}_2$ as a $\mathbb{Z}_2$-module. Thus $\lambda^\delta = 1+4\mu$ for some $\mu \in \mathbb{Z}_2$, $\mu \neq 0$. Now, $\sigma^\delta \tau^\gamma \sigma^{-\delta} = \tau^\gamma$ implies that $\tau^\gamma = \tau^{\gamma(1+4\mu)}$ and so $\tau^{4\mu\gamma} = 1$, what is impossible. Thus the *claim* is proved.

Now, let $\lambda = 1+4\nu$, $\nu \neq 0$ and $t = \sigma^\alpha \tau^\beta \in T$, $\alpha, \beta \in \mathbb{Z}_2$. If $\alpha, \beta \neq 0$, then $t^{-1}\sigma t \sigma^{-1} = (\tau^{-\beta}\sigma^{-\alpha})(\sigma\sigma^\alpha\tau^\beta\sigma^{-1}) = \tau^{-\beta}(\sigma\tau\sigma^{-1})^\beta = \tau^{-\beta}\tau^{\beta+4\nu\beta} = \tau^{4\nu\beta} \in T \cap \langle\tau\rangle = \langle\tau^{2^r}\rangle$, for some integer $r \geqslant 0$. If $\beta = 0$ and $\alpha \neq 0$, let $\lambda^\alpha = 1+4\mu$, $\mu \neq 0$. Then $\tau^{-1}t\tau t^{-1} = \tau^{-1}\sigma^\alpha\tau\sigma^{-\alpha} = \tau^{4\mu} \in T \cap \langle\tau\rangle = \langle\tau^{2^r}\rangle$, for some integer $r \geqslant 0$. Consequently, $\alpha \neq 0$ implies that there exists integer $r \geqslant 0$ such that $T \cap \langle\tau\rangle = \langle\tau^{2^r}\rangle$. The last equality implies that $\tau^{2^r} = t\tau^{2^r}t^{-1} = \sigma^\alpha\tau^{2^r}\sigma^{-\alpha}$, contradicting the claim. Hence $\alpha = 0$ and $T \subseteq \langle\tau\rangle$. Finally, if $(\langle\tau\rangle : T) = 2^r$, then $G/T \cong (\mathbb{Z}/2^r\mathbb{Z}) \rtimes \mathbb{Z}_2$. So $G/T \cong \mathbb{Z}_2$ yields $T = \langle\tau\rangle$.

In the proof of the next lemma we shall follow the arguments presented in [11, Proposition 4.6].

Let $a \in K^*$, we shall denote by $a^{1/2^s}$ a suitably fixed 2^sth root of a such that $(a^{1/2^{s+1}})^2 = a^{1/2^s}$. In case $a = 1$ we call $\varepsilon_s = a^{1/2^s}$, and it is a primitive 2^sth root of 1. We shall also use the notation $i = \varepsilon_2$.

3.3. Lemma. *Let K be a C-field, which is not formally real, such that $|K^*/q(K)| = 4$, $\varepsilon_r \notin K$ and $\varepsilon_{r-1} \in K$ for some $r \geqslant 2$. Let L be the field obtained from K by adjoining ε_n for all $n \geqslant 1$. Then*:

(a) *If $r = 2$ and $L = K(i)$, then $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$ and we can choose generators σ and τ for the $\mathbb{Z}_2$ components such that $\sigma\tau\sigma^{-1} = \tau^{-1}$.*

(b) *Otherwise $G(L; K) \cong \mathbb{Z}_2$. Further, if $r = 2$, then $\varepsilon_3 \in K(i)$.*

Proof. Following [19, Sect. 4] let us give a general description of L. Recall that we can write $\varepsilon_n = (\xi_n + i\eta_n)/2$ for $n \geqslant 1$, where $\xi_n = \varepsilon_n + \varepsilon_n^{-1}$ and $\eta_n = -i(\varepsilon_n - \varepsilon_n^{-1})$. Hence $\xi_n^2 = (\varepsilon_n + \varepsilon_n^{-1})^2 = \varepsilon_n^2 + \varepsilon_n^{-2} + 2 = \varepsilon_{n-1} + \varepsilon_{n-1}^{-1} + 2 = \xi_{n-1} + 2$, for $n \geqslant 2$. In the same way we get $\eta_n^2 = 2 - \xi_{n-1}$, for $n \geqslant 2$. On the other hand $\xi_n\eta_n = -i(\varepsilon_n + \varepsilon_n^{-1})(\varepsilon_n - \varepsilon_n^{-1}) = -i(\varepsilon_n^2 - \varepsilon_n^{-2}) = -i(\varepsilon_{n-1} - \varepsilon_{n-1}^{-1}) = \eta_{n-1}$ for $n \geqslant 2$. From these relations it follows that the sequence of fields defined by $K_n = K(i, \xi_n)$, for $n \geqslant 2$, satisfies the conditions: $K_n \subseteq K_{n+1}$, $K_n = K_2(\eta_n)$ and $L = \bigcup K_n$, for $n \geqslant 2$. Finally, if $L \neq K_2$, then [19, Lemma 4.2] yields $t > 2$ such that for every $m \geqslant 0$, K_{t+m+1} is the only quadratic extension of K_{t+m} in L. Therefore $G(L; K_2) \cong \mathbb{Z}_2$, whenever $L \neq K_2$. Now, returning to the proof of Lemma 3.3, let us prove (a).

By [18, Corollary 2.10], K_2 is also a C-field and also K_2 has four square classes, by [18, Corollary 3.12]. Next, take $a \in K^* - \pm q(K)$. By [12, Theorem 3.4, p. 202], $a \notin q(K_2)$. On the other hand we have $-1 = c^2 + d^2$ with $c, d \in K^*$, by [18, Proposition 1.1]. Since $c^2 + d^2 = (c+id)(c-id)$, then $c+id \notin q(K_2)$. A direct verification shows that $b \notin aq(K_2)$. Hence, 1, a, $c+id$, $a(c+id)$ represent the distinct square classes of K_2^*. Therefore [18, Corollary 3.9-(1)] implies that $K(2) = K_2(\{a^{1/2^n}, (c+di)^{1/2^n} \mid n \geq 1\})$.

Let us call $N = K_2(\{(c+di)^{1/2^n} \mid n \geq 1\})$. First of all observe that $f(X) = [X^{2^n} - (c+di)][X^{2^n} - (c-di)] = X^{2^{n+1}} - 2cX^{2^n} - 1$ is the minimal polynomial of $c+di$ over K. Next observe that $[(c+di)^{1/2^n}(c-di)^{1/2^n}]^{2^n} = -1$. Hence $(c-di)^{1/2^n} = \varepsilon_{n+1}^j (c+di)^{1/2^n}$ for some j. Thence $K_2((c+di)^{1/2^n})$ is the normal extension of K generated by the roots of $f(X)$. Thus the field N above is a normal extension of K. It is easy to see that $G(N; K_2) \cong \mathbb{Z}_2$. Let us now call $F = K(\{a^{1/2^n} \mid n \geq 1\})$. It is clear from our construction that $N \cap F = K$ and $NF = K(2)$.

To finish the proof we take an N-automorphism τ such that $\tau(a^{1/2^n}) = \varepsilon_n a^{1/2^n}$ for every $n \geq 1$ and an F-automorphism σ such that $\sigma((c+di)^{1/2^n}) = (c-di)^{1/2^n}$. It is easy to see that σ and τ are the desirable generators.

(b) If $r > 2$, then $K = K_2$ and as we have already observed $G(L; K) \cong \mathbb{Z}_2$. For the last case let $m \geq 2$ be an integer such that $\varepsilon_m \in K_2 = K(i)$ and $\varepsilon_{m+1} \notin K_2$. Hence $\xi_{m+1}, \eta_{m+1} \notin K_2$, as was observed in the beginning of the proof. Suppose that $G(L; K)$ is not a cyclic group. Thus $G(L; K) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ and for every $n \geq m+1$, $K(\xi_n)$ is a cyclic extension of K in L of degree 2^{n-m}. Since K has just three quadratic extensions, they are K_2, $K(\xi_{m+1})$ and $K(i\xi_{m+1})$, all of them are contained in L. Call $N = K(\xi_{m+1})$. By [18, Corollary 2.10] N is also a C-field and by [18, Corollary 3.12] N has also four square classes. Hence N has three quadratic extensions, namely $N(i) = K_2(\xi_{m+1}) = K_{m+1}$, $N(\xi_{m+2}) = K(\xi_{m+2})$, and $N(i\xi_{m+2}) = K(i\xi_{m+2})$. Observe that if $\xi_{m+1}^{1/2} \in K_2(\xi_{m+1})$, then $\xi_{m+1} \in K_2$ contradicting our assumption. Thus $N(\xi_{m+1}^{1/2}) = K(\xi_{m+2})$ or $N(\xi_{m+1}^{1/2}) = K(i\xi_{m+2})$. In both cases $N(\xi_{m+1}^{1/2})$ is a Galois extension of K. Therefore, $N(\xi_{m+1}^{1/2})$ contains the roots of the minimal polynomial $X^4 - (2+\xi_m)$ of $\xi_{m+1}^{1/2}$ over K. Since the zeros of this polynomial are $\pm\rho$, $\pm i\rho$, for some $\rho \in K(2)$, it follows that $i \in N(\xi_{m+1}^{1/2})$. However, this is impossible, since $N(i)$, $K(\xi_{m+2})$ and $K(i\xi_{m+2})$ are distinct quadratic extensions of N.

To complete the proof observe that if $\varepsilon_3 \notin K_2$, then $2^{1/2} = \xi_3 \notin K_2$ and so $K(2^{1/2}) \neq K_2$. Since $K(2^{1/2}) \subset L$ it follows that K_2 is not the only quadratic extension of K in L and then $G(L; K)$ is not a cyclic group. ∎

Let us recall that a field is called of *Class C*, or a *C-field*, if $B(K) = \pm q(K)$ ([18, Definition 1.10]).

3.4. THEOREM. *Let K be a field such that $G(K)$ is a non-abelian group that contains a normal subgroup U, with $U \cong \mathbb{Z}_2$ and $C(U) = U$. Then K is a C-field, $(K^* : q(K)) = 4$, $B(K) \neq K^*$ and $G(K) = \langle \tau \rangle \rtimes \langle \sigma \rangle$, where K, τ and σ satisfy one of the following conditions*:

(a) *K is a formally real field which is hereditarily-pythagorean with respect to $K(2)$ (see [3, Chap. III, p. 86]). Moreover, K has two orderings, $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ and $\sigma^2 = 1$ and $\sigma\tau\sigma = \tau^{-1}$.*

(b) *$-1 \notin q(K)$ and there exists $m \geq 2$ such that $\varepsilon_{m+1} \in K(i)$ and $\varepsilon_{m+2} \notin K(i)$. In this case $\sigma\tau\sigma^{-1} = \tau^{2^m-1}$ and $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$.*

(c) *There exists $m \geq 2$ such that $\varepsilon_m \in K$ and $\varepsilon_{m+1} \notin K$. In this case $\sigma\tau\sigma^{-1} = \tau^{2^m+1}$ and $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$.*

Proof. Since $C(U) = U$ if $\varphi: G(K) \to \mathrm{Aut}(U) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ is the homomorphism given by $\varphi(g)(u) = gug^{-1}$, for every $g \in G(K)$ and $u \in U$, we have that $\mathrm{kernel}(\varphi) = C(U) = U$. Therefore, $G(K)$ is metabelian (see [19, p. 235]), and for every $u \in U$ $gug^{-1} = u^{\alpha}$ for some $\alpha \in \{\pm 1\} \times (1 + 4\mathbb{Z}_2) = \mathrm{Aut}(U)$.

By [19, Theorem 4.5] K is a C-field and so $B(K) = \pm q(K)$ by [18, Theorem 1.9] as desired.

Since $\mathrm{image}(\varphi) \subseteq \mathrm{Aut}(U)$ there are three cases to be examined.

Case 1. $\mathrm{Image}(\varphi) = \{\pm 1\}$.

Let $\sigma \in \varphi^{-1}(-1) \subseteq G(K)$. Then $\sigma u \sigma^{-1} = u^{-1}$ for every $u \in U$ and $\varphi(\sigma)^2 = 1$ yields $\sigma^2 \in U$. Thus $(\sigma^2)^{-1} = \sigma(\sigma^2)\sigma^{-1} = \sigma^2$ implies $\sigma^2 = 1$, and σ is an involution of $G(K)$. Hence the exact sequence $1 \to U \to G(K) \to \{\pm 1\} \to 1$ splits and $G(K)$ is the semidirect product of U by $\langle\sigma\rangle$. Now, consider a generator τ of U, then $\sigma\tau\sigma^{-1} = \tau^{-1}$, as desired. Moreover, $(K^* : q(K)) = 2^{r(G(K))} = 4$. Since σ and $\sigma\tau$ are involutions, and they are not in the same conjugacy class, the field K is a formally real field having at least two different orderings [3, Chap. II, Theorem 4, p. 78]. Since K has four square classes, then it has exactly two orderings and so Case 1 yields (a).

Case 2. $\mathrm{Image}(\varphi) \subseteq (1 + 4\mathbb{Z}_2)$.

In this case the $\mathrm{image}(\varphi) \cong \mathbb{Z}_2$ is a free pro-2-group and we have the split exact sequence $1 \to U \to G(K) \to \mathbb{Z}_2 \to 1$. Hence $G(K) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$ and $(K^* : q(K)) = 2^{r(G(K))} = 4$ as required.

Let L be the field obtained from K by adjoining all 2^nth roots of 1 for all $n \geq 1$. By Lemma 3.3(a) if $i \notin K$ and $L = K(i)$, then $G(K) = \langle\tau\rangle \rtimes \langle\sigma\rangle$ where $\sigma\tau\sigma^{-1} = \tau^{-1}$. Thus $G(K(i)) = \langle\tau\rangle \times \langle\sigma^2\rangle$ is an abelian subgroup of $G(K)$ not contained in $U \cong \mathbb{Z}_2$. But this contradicts Lemma 3.2. Hence $G(L; K) \cong \mathbb{Z}_2$ by Lemma 3.3(b). On the other hand [19, Theorem 4.1] implies that $G(L)$ is also an abelian group. Applying again Lemma 3.2 we get $U = G(L)$ since $G(L; K) \cong \mathbb{Z}_2$.

Suppose first that $-1 \notin q(K)$. By Lemma 3.3(b), $\varepsilon_3 \in K(i)$. By [18, Corollary 2.10], $K(i)$ is a C-field and by Lemma 3.2, $G(K(i))$ is not an abelian group. Thus Theorem 3.6 of [18] implies that there exists $s \geq 1$ such that $\varepsilon_s \notin K(i)$. Thus, there is $m \geq 2$ such that $\varepsilon_{m+1} \in K(i)$ and

$\varepsilon_{m+2} \notin K(i)$. Let $a \in K^* - \pm q(K)$ and let $F = K(\{a^{1/2^n} | n \geqslant 1\})$. Since F is not a finite extension of K we have $LF = K(2)$. Since $K(i)$ is the unique quadratic extension of K inside L and $-1 \notin q(F)$ it follows that $L \cap F = K$. Therefore, $G(F) \cong G(L; L \cap F) \cong \mathbb{Z}_2$ and $K(2) = L(\{a^{1/2^n} | n \geqslant 1\})$. On the other hand $K(2)$ is also the field obtained from F by adjoining ε_n for all $n \geqslant 1$. Again, from $L \cap F = K$ it follows that $\varepsilon_{m+1} \in F(i)$ and $\varepsilon_{m+2} \notin F(i)$. Now, observe that for the non-trivial F-automorphism σ of $F(i)$ we have that $\varepsilon_{m+1}\sigma(\varepsilon_{m+1}) \in F$ and $(\varepsilon_{m+1}\sigma(\varepsilon_{m+1}))^{2^{m+1}} = 1$. Thus $\varepsilon_{m+1}\sigma(\varepsilon_{m+1}) = \pm 1$ and $\sigma(\varepsilon_{m+1}) = \pm\varepsilon_{m+1}^{-1}$. If $\sigma(\varepsilon_{m+1}) = \varepsilon_{m+1}^{-1}$, we must have $\xi_{m+1} \in F$. Since $\varepsilon_{m+2} \notin F(i)$ we must have $\xi_{m+2} \notin F(i)$, as well. Thus $F(\xi_{m+2})$ is also a quadratic extension of F in $K(2)$ and it is different from $F(i)$. But this cannot occur since $G(F)$ is a cyclic group. Hence $\sigma(\varepsilon_{m+1}) = -\varepsilon_{m+1}^{-1}$. On the other hand, since $\varepsilon_n = \varepsilon_{m+1}^{2^{m-n+1}}$ for every $1 \leqslant n \leqslant m$, we have that $\sigma(\varepsilon_n) = \varepsilon_n^{-1}$ for every $1 \leqslant n \leqslant m$.

Now, lift σ to an F-automorphism σ of $K(2)$ such that $\sigma(\varepsilon_n) = \varepsilon_n^{2^m - 1}$ for every $n \geqslant 1$. This is possible because $\sigma(\varepsilon_n) = \varepsilon_n^{-1} = \varepsilon_n^{2^n - 1} = \varepsilon_n^{2^m - 1}$ for $1 \leqslant n \leqslant m$. And for $n > m$, $n = m + r$ for some $r \geqslant 1$, once again $\sigma(\varepsilon_n) = \sigma(\varepsilon_{m+r}) = \varepsilon_{m+r}^{2^m - 1}$. Next, take an L-automorphism τ such that $\tau(a^{1/2^n}) = \varepsilon_n a^{1/2^n}$ for every $n \geqslant 1$. It is immediate that $\sigma\tau\sigma^{-1} = \tau^{2^m - 1}$ and so we have (b).

Assume now that $\varepsilon_m \in K$, and $\varepsilon_{m+1} \notin K$, for $m \geqslant 2$, then $K^* = q(K) \cup \varepsilon_m q(K) \cup aq(K) \cup a\varepsilon_m q(K)$ for some $a \in K^*$. Let $F = K(\{a^{1/2^n} | n \geqslant 1\})$. As above $LF = K(2)$ and $L \cap F = K$. Once again we can choose an F-automorphism σ and an L-automorphism τ such that $\sigma(\varepsilon_n) = \varepsilon_n^{2^m + 1}$ and $\tau(a^{1/2^n}) = \varepsilon_n a^{1/2^n}$, for $n \geqslant 1$ (observe that $\sigma(\varepsilon_n) = \varepsilon_n = \varepsilon_n^{2^m + 1}$ for every $1 \leqslant n \leqslant m$). Thus $\sigma\tau\sigma^{-1} = \tau^{2^m + 1}$ and we have (c).

Case 3. $\mathrm{Image}(\varphi) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

In this case let us take $S = \varphi^{-1}(\mathbb{Z}/2\mathbb{Z})$. S is a normal subgroup of $G(K)$ such that $U \subseteq S$ and $|\varphi(S)| = 2$. Clearly the centralizer of U in S is U, as well. Hence, as in the proof of Case 1, $S = U \rtimes \langle\sigma\rangle$, for some involution $\sigma \in G(K)$. Thus K is a formally real field, and since it is a C-field, $G(K) \cong \mathbb{Z}_2^\alpha \rtimes \mathbb{Z}/2\mathbb{Z}$, by [3, Theorem 15, p. 118]. Therefore, if $\alpha \neq 1$ we have a contradiction to $C(U) = U$, and if $\alpha = 1$ we have a contradiction to image $(\varphi) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. Hence, this last case does not occur and the proof is finished. ∎

3.5. Corollary. *Let K be a field such that $G(K)$ is described either by* (b) *or by* (c) *above. Then K fulfills the hypothesis of Theorem* 2.10 *and $G^T(\tilde{O}(K); K)$ is the largest abelian normal subgroup of $G(K)$.*

Proof. In case (b) we have that $(K^* : B(K)) = 2$ and K is not an exceptional field. Hence Proposition 2.11 yields the existence of $O(K)$. By Theorem 2.10(a), $O(K)^* q(K) = B(K) = \pm q(K)$. Thus $\mathscr{K}^*_{O(K)} = q(\mathscr{K}_{O(K)}) \cup -q(\mathscr{K}_{O(K)})$. Thence $G(\mathscr{K}_{O(K)}) \cong \mathbb{Z}_2$. By Theorem 2.10(c), $G^T(\tilde{O}(K); K)$ is a normal abelian subgroup of $G(K)$ of rank 1. Since $G(K)/G^T(\tilde{O}(K); K) \cong G(\mathscr{K}_{O(K)})$, Lemma 3.2 yields the desired conclusion.

Next, in case (c) we see that $B(K) = q(K)$ and so $(K^* : B(K)) = 4$. Proposition 2.11 therefore implies that K fulfills the desired assumption. Since $\varepsilon_m \in K$ and $\varepsilon_{m+1} \notin K$, the same holds for $\mathscr{K}_{O(K)}$ because $O(K)$ is a 2-henselian valuation ring. Thus $\mathscr{K}_{O(K)}(2)$ is the field obtained from $\mathscr{K}_{O(K)}$ by adjoining ε_n for all $n \geq 1$ and so $G(\mathscr{K}_{O(K)}) \cong \mathbb{Z}_2$. Now, we can finish the proof arguing as in case (b). ∎

3.6. *Remarks.* (a) By [11, Section 5] there are fields having $G(K)$ as described in Theorem 3.4.

(b) In case (a) of Theorem 3.4 we do not have in general the existence of a proper 2-henselian valuation ring. For example:

(b-1) By [4], or by [17, p. 85], there exists an algebraic extension K of the rationals $\mathbb{Q}$ for which the statements of case (a) of the Theorem hold. Since K has only archimedean orders we know by [8, Proposition 6] that K does not have proper henselian valuation rings. Let Ω be an algebraic closure of $\mathbb{Q}$ that contains K. Since $G(\Omega; K(i)) = \langle \tau \rangle$ is a cyclic group we have for every valuation ring C of Ω that either $K^Z(C; K(i)) = \Omega$ or $K^Z(C; K(i))$ is a finite extension of $K(i)$ and then of K, too. By [10, Theorem 3.11 and Theorem 3.15], $K^Z(C; K(i))$ is not a finite extension of K for every valuation ring C of Ω. Thus $K^Z(C; K) = \Omega$. By [7, (15.6)-c)], $K^Z(C \cap K(2); K) = K^Z(C; K) \cap K(2) = K(2)$, for every valuation ring C of Ω. Then there is no proper 2-henselian valuation ring of K.

(b-2) On the other hand if $K = \mathbb{R}((X))$, the power series field over $\mathbb{R}$, then K is also as in case (a). Denote $\mathbb{R}[[X]] = A$. Then $A \in \mathscr{H}(\mathbb{R}((X)))$, $\mathscr{K}_A = \mathbb{R}$ and $\Gamma_A = \mathbb{Z}$. Hence $O(K) \subseteq A$ by Theorem 2.10(e). Since $\mathscr{H}(\mathbb{R}) = \{\mathbb{R}\}$, it follows that $O(K) = \mathbb{R}[[X]]$ and $G^T(\tilde{O}(K); K) = G(K(i))$ is the largest abelian normal subgroup of $G(K)$.

(c) Theorem 3.4 also shows that the study of abelian normal subgroups of $G(K)$ for fields K of characteristic two is not interesting. More specifically, if K is a field such that $c(K) = 2$, then $G(K)$ is a free pro-2-group by [15, Corollary 3.4, p. 257]. Therefore, $U \cong \mathbb{Z}_2$ for every non-trivial abelian subgroup U of $G(K)$. In particular, $U \cong \mathbb{Z}_2$ if U is an abelian normal subgroup and $C(U) = U$ by Proposition 3.1. This contradicts Theorem 3.4, if $G(K)$ has rank $\neq 1$.

4. The General Case

In [18] Ware proved that the class of C-fields K that contains all the 2^nth roots of unity, $n \geq 1$, is the same as the class of fields such that $G(K)$

is an abelian group. Becker [3] stated a similar result for formally real C-fields K proving that they are the fields for which $G(K(i))$ is an abelian group. In this section we shall examine the existence of normal abelian subgroups of $G(K)$ for arbitrary fields K.

Recall that a C-field (or a field of class C [18], or rigid field [20]) is a field K such that $B(K) = \pm q(K)$. A C-field which is formally real is also called superpythagorean by Elman and Lam (see [13, Appendix to Sect. 5, p. 44]). By [13, Corollary 5.16, p. 46] the superpythagorean fields are the fields hereditarily pythagorean with respect to $K(2)$ (see also [3, Chap. III, p. 86]). Since a formally real C-field K is pythagorean we see that K is an exceptional field (see Definition 2.9). Conversely, a formally real exceptional field K is hereditarily pythagorean with respect to $K(2)$ and so a C-field. This is not the case for non-formally real fields, since there exist non-formally real C-fields K for which $-1 \notin q(K)$.

Let us now start our discussion recalling the following theorem of Ware:

4.1. THEOREM [18, Theorem 3.6]. *For a field K with $(K^* : q(K)) > 2$ the following statements are equivalent*:

(a) *$B(K) = q(K)$ and $\varepsilon_n \in K$ for all $n \geq 1$.*

(b) *$G(K)$ is an abelian group.* ▮

4.2. COROLLARY. *Let K be a field satisfying the above equivalent conditions. Then K fulfills the hypothesis of Theorem 2.10 and $G(K) = G^T(\tilde{O}(K); K)$ or $G(K) = G^T(\tilde{O}(K); K) \times \mathbb{Z}_2$.*

Proof. Proposition 2.11 yields the existence of $O(K)$ and by Theorem 2.10 we know that $O(K)$ is a non-dyadic valuation ring of K. Moreover, $G(\mathscr{K}_{O(K)})$ is also an abelian group since $G(\mathscr{K}_{O(K)}) \cong G(K)/G^T(\tilde{O}(K); K)$, by [7, Corollary 19.9].

To end the proof we *claim* that $(\mathscr{K}^*_{\tilde{O}(K)} : q(\mathscr{K}_{O(K)})) \leq 2$.

By the claim, $G(K) = G^T(\tilde{O}(K); K)$ if $\mathscr{K}^*_{\tilde{O}(K)} = q(\mathscr{K}_{O(K)})$ while $G(K) = G^T(\tilde{O}(K); K) \times \mathbb{Z}_2$ if $(\mathscr{K}^*_{\tilde{O}(K)} : q(\mathscr{K}_{O(K)})) = 2$.

Assume now that $(\mathscr{K}^*_{\tilde{O}(K)} : q(\mathscr{K}_{O(K)})) > 2$, contrary to the claim. Hence the above theorem implies that $B(\mathscr{K}_{O(K)}) = q(\mathscr{K}_{O(K)})$. So $(\mathscr{K}^*_{\tilde{O}(K)} : B(\mathscr{K}_{O(K)})) > 2$, which contradicts Theorem 2.10(b). ▮

The first two examples presented in 4.11 show that both possibilities may occur and Theorem 4.5(a) describes a family of fields K for which $G(K(i)) = G^T(\tilde{O}(K); K) \times \mathbb{Z}_2$.

The next result will simplify the proof of Theorem 4.4.

4.3. LEMMA. *Let K be a field such that $(K^* : q(K)) > 2$, and $G(K)$ contains a non-trivial normal abelian subgroup U. Then $B(K) \neq K^*$.*

Proof. If $G(K)$ is an abelian group it follows from Theorem 4.1 that $B(K)=q(K)\neq K^*$. Assume now that $G(K)$ is a non-abelian group and $U\cong\mathbb{Z}_2$. If there exists a normal subgroup U' of G such that $U\subseteq U'$, $U'\cong\mathbb{Z}_2$ and $C(U')=U'$, the result follows from Theorem 3.4. Otherwise, Proposition 3.1(b) yields the existence of a subgroup S of $G(K)$ such that $U\subseteq S$ and $S\cong\mathbb{Z}_2\times\mathbb{Z}_2$. Let E and F be the fixed fields of U and S, respectively. Then $(F^*:q(F))=4$ and by Theorem 4.1 $B(F)=q(F)$. Therefore, by Proposition 2.11 and Theorem 2.10, we get that $O(F)$ is a proper, non-dyadic, 2-henselian valuation ring of F. Now we see that E, F and $C=O(F)$ satisfy the conditions of Corollary 2.16. Thus $B(K)\neq K^*$ by Theorem 2.10(b).

Let us consider now U with $r(U)>1$. Let E be the fixed field of U. Since $r(U)>1$, $B(E)=q(E)$ by Theorem 4.1. Then, by Proposition 2.11 and Theorem 2.10, we get that $O(E)$ is a proper, non-dyadic, 2-henselian valuation ring of E. Since $F=E$, and $C=O(E)$ satisfy the conditions of Corollary 2.16, Theorem 2.10(b) yields again $B(K)\neq K^*$. ∎

We now give a generalization of Ware's Theorem for non-C-fields. Recall that a non-C-field is also a non-exceptional field.

4.4. THEOREM. *Let K be a non-C-field such that $B(K)\neq K^*$. Then K fulfills the hypothesis of Theorem* 2.10 *and $G^T(\tilde{O}(K); K)$ is the largest normal abelian subgroup of $G(K)$. Furthermore, $r(G^T(\tilde{O}(K); K))=r(K^*/B(K))$.*

Proof. Proposition 2.11 implies the existence of $O(K)$. By Theorem 2.10(c) we have that $G^T(\tilde{O}(K); K)$ is a normal abelian subgroup of $G(K)$ and $r(G^T(\tilde{O}(K); K))=r(K^*:O(K)^*\,q(K))$. Moreover, $r(K^*:O(K)^*\,q(K))=r(K^*:B(K))$ since $B(K)=O(K)^*\,q(K)$ by 2.10(a).

Now let U be a normal abelian subgroup of $G(K)$. We have two cases:

Case 1. $U\cong\mathbb{Z}_2$. Let F be the fixed field of U. By [7, 19.10] we have that $G^T(\tilde{O}(K); F)=G^T(\tilde{O}(K); K)\cap U$. The diagram illustrating the position of the fixed fields of these groups is as follows:

$$\begin{tikzcd}[column sep=small]
& K(2) \arrow[d, dash] & & \\
& K^T(\tilde{O}(K);F) \arrow[dl, dash] \arrow[dr, dash] \arrow[rr, dotted, dash] & & G^T(\tilde{O}(K);K)\cap U \\
F \arrow[dr, dash] & & K^T(\tilde{O}(K);K) \arrow[dl, dash] \arrow[r, dotted, dash] & G^T(\tilde{O}(K);K) \\
& F\cap K^T(\tilde{O}(K);K) \arrow[d, dash] \arrow[rr, dotted, dash] & & UG^T(\tilde{O}(K);K) \\
& K & &
\end{tikzcd}$$

By [7, Corollary 19.9] we know that the index $(G(F) : G^T(\tilde{O}(K); F))$ cannot be a finite number unless $G(F) = G^T(\tilde{O}(K); F)$. We can therefore conclude that either $G^T(\tilde{O}(K); K) \cap U = \{1\}$ or $U \subseteq G^T(\tilde{O}(K); K)$.

If $G^T(\tilde{O}(K); K) \cap U = \{1\}$, or equivalently $K^T(\tilde{O}(K); F) = K(2)$, we have that $UG^T(\tilde{O}(K); K)/G^T(\tilde{O}(K); K) \cong U/U \cap G^T(\tilde{O}(K); K) \cong U \cong \mathbb{Z}_2$. Now, recall that

$$UG^T(\tilde{O}(K); K)/G^T(\tilde{O}(K); K) \cong G(K^T(\tilde{O}(K); K); F \cap K^T(\tilde{O}(K); K)).$$

By [7, Theorem 19.13] this last group is isomorphic to $G(\mathscr{K}_{O(K)}(2); \mathscr{K})$, where $\mathscr{K}$ is the residue class field of $\tilde{O}(K) \cap (F \cap K^T(\tilde{O}(K); K))$. Thus $\mathbb{Z}_2 \cong G(\mathscr{K}(2); \mathscr{K})$ is a normal subgroup of $G(\mathscr{K}_{O(K)})$.

We now *claim* that $(\mathscr{K}^*_{\tilde{O}(K)} : q(\mathscr{K}_{O(K)})) > 2$.

The claim and Lemma 4.3 show that $B(\mathscr{K}_{O(K)}) \neq \mathscr{K}^*_{\tilde{O}(K)}$. This contradicts Theorem 2.10(b), since K is non-exceptional. Thus $U \subseteq G^T(\tilde{O}(K); K)$ as desired.

Proof of the Claim. If $(\mathscr{K}^*_{\tilde{O}(K)} : q(\mathscr{K}_{O(K)})) = 1$, then $O(K) \in \mathscr{H}_2(K)$ which yields $B(K) = q(K)$, by Proposition 2.12. But this cannot occur since K is a non-C-field.

Let us assume now $(\mathscr{K}^*_{\tilde{O}(K)} : q(\mathscr{K}_{O(K)})) = 2$. Thus $G(\mathscr{K}_{O(K)}(2); \mathscr{K}_{O(K)}) \cong \mathbb{Z}_2$. Hence $\mathscr{K}$ is a finite extension of $\mathscr{K}_{O(K)}$ and so $F \cap K^T(\tilde{O}(K); K)$ is also a finite extension of K. Since $U (= G(F))$ and $G^T(\tilde{O}(K); K)$ are normal abelian subgroups of $G(K)$ with trivial intersection, $G(F \cap K^T(\tilde{O}(K); K)) \cong G(F) \times G^T(\tilde{O}(K); K)$ is an abelian group. Consequently, by Theorem 4.1 $F \cap K^T(\tilde{O}(K); K)$ is a C-field (since $r(G(F \cap K^T(\tilde{O}(K); K))) > 1$ by the above isomorphism). By [18, Corollary 2.11] K is also a C-field, a contradiction. Hence the *claim* is true.

Case 2. Assume now that $r(U) > 1$. Let F be the fixed field of U and $C = \tilde{O}(K) \cap F$.

(A) If $C \in \mathscr{H}_2(F)$, we will show that $G(F) = G^T(\tilde{C}; F) = G(F) \cap G^T(\tilde{O}(K); K)$. Since C is non-dyadic and $C \in \mathscr{H}_2(F)$ it follows that $\mathscr{K}_C = \mathscr{K}_C(2)$. Hence $G(F) = G^T(\tilde{C}; F)$ by [7, 19.9] and by [7, 19.1-(b)] $G^T(\tilde{C}; F) = G(F) \cap G^T(\tilde{O}(K); K)$. Thus $U = G(F) \subseteq G^T(\tilde{O}(K); K)$ as required.

(B) Assume that $C \notin \mathscr{H}_2(F)$ and let $A = O(F) \cap K$. Observe that $c(\mathscr{K}_A) = c(\mathscr{K}_{O(F)}) \neq 2$. Since $O(F)$ has no non-trivial convex 2-divisible subgroup the same is true for A, by Proposition 2.13.

First let us prove that $A \notin \mathscr{H}(K)$. If $A \in \mathscr{H}(K)$, then $O(K) \subseteq A$ by Theorem 2.10(e). Hence $C \subseteq O(F)$ and Proposition 2.12(b) implies that $G^T(\tilde{O}(K); F) = G^T(\tilde{O}(F); F)$ (recall that $\tilde{O}(K) = \tilde{C}$). Moreover, $C \notin \mathscr{H}_2(F)$ and $C \subseteq O(F)$ show that $O(F) \notin \mathscr{H}_2(F)$ and then $G(F) \neq G^T(\tilde{O}(F); F)$.

Hence $G(F)=G^T(\tilde{O}(F); F)\times\mathbb{Z}_2$, by Corollary 4.2. Consequently, $G(F)=G^T(\tilde{O}(K); F)\times\mathbb{Z}_2$ and we are in the situation illustrated in the diagram in Case 1. As before let us call $\mathscr{K}$ the residue class field of $\tilde{O}(K)\cap(F\cap K^T(\tilde{O}(K); K))$. Thus $\mathbb{Z}_2\cong G(\mathscr{K}(2);\mathscr{K})$ is a normal subgroup of $G(\mathscr{K}_{O(K)})$. Assume now $(\mathscr{K}^*_{\tilde{O}(K)}:q(\mathscr{K}_{O(K)}))>2$. Hence $B(\mathscr{K}_{O(K)})\neq\mathscr{K}^*_{\tilde{O}(K)}$ by Lemma 4.3 which contradicts Theorem 2.10(b), since K is non-exceptional.

If $(\mathscr{K}^*_{\tilde{O}(K)}:q(\mathscr{K}_{O(K)}))=1$, arguing as in the Case 1 we get that K is a C-field, contrary to one of theorem's hypotheses. For the case $(\mathscr{K}^*_{\tilde{O}(K)}:q(\mathscr{K}_{O(K)}))=2$, we argue as in the Case 1 and we get that $F\cap K^T(\tilde{O}(K); K)$ is also a finite extension of K. Now, since $U=G(F)$ is an abelian group of rank >2, $\varepsilon_n\in F$ for all $n\geqslant 1$ and so $\varepsilon_n\in F\cap K^T(\tilde{O}(K); K)$ for all $n\geqslant 1$. In particular $-1\in F\cap K^T(\tilde{O}(K); K)$ and $\mathscr{K}^*=q(\mathscr{K})\cup\bar{u}q(\mathscr{K})$, for some $u\in\tilde{O}(K)\cap(F\cap K^T(\tilde{O}(K); K))$, $\bar{u}\notin\pm q(\mathscr{K})=q(\mathscr{K})$. Hence $B(\mathscr{K})=q(\mathscr{K})$ and by [1, Proposition 1.5] $B(F\cap K^T(\tilde{O}(K); K))=q(F\cap K^T(\tilde{O}(K); K))$, too. So $F\cap K^T(\tilde{O}(K); K)$ is a C-field and again K is a C-field by [18, Corollary 2.11], a contradiction.

Therefore $A\notin\mathscr{H}(K)$ and then by Theorem 2.15 there exists a valuation ring D of F such that $O(F)\subset D$, $D\cap K\in\mathscr{H}(K)$ and $G(F)\subseteq G^T(\tilde{D}; K)$. Next, we want to show that D may be chosen so that $D\subseteq C$. By Proposition 2.12(b), C and $O(F)$ are comparable valuation rings. Since $C\subseteq O(F)$ implies $O(K)=C\cap K\subseteq O(F)\cap K=A$, which forces $A\in\mathscr{H}(K)$, we see that $O(F)\subseteq C$. Thus Theorem 2.15 yields D as desired. Since $O(F)\subset D$ is a non-dyadic valuation ring, so is D. Hence $G^T(\tilde{D}; K)=G^T(\tilde{O}(K); K)$ by Proposition 2.12(b). (Recall that $\tilde{D}$ is the unique extension of $D\cap K$ to $K(2)$.) Thus $U=G(F)\subseteq G^T(\tilde{O}(K); K)$ as required. ∎

We now generalize Theorem 3.4 and Corollary 3.5 for C-fields, non-formally real and not containing all the 2^nth roots of the unity. The result is also a complement to results 4.1 and 4.3 of [19].

We first introduce some conventions that will simplify the statements of the theorem. Let K be a field for which the valuation ring $O(K)$ already exists, Λ be a set of indices of cardinality $r(K^*/O(K)^*q(K))$ and $\{a_\lambda\mid\lambda\in\Lambda\}\subset K^*$ be an $\mathbb{F}_2$-basis of $K^T(\tilde{O}(K); K)$ modulo $q(K^T(\tilde{O}(K); K))$ as stated by Theorem 2.10(c). Then $K(2)$ is the field obtained from $K^T(\tilde{O}(K); K)$ by adjoining all 2^nth roots of a_λ for all $n\geqslant 1$ and $\lambda\in\Lambda$ by Theorem 4.1 and [18, Corollary 3.9-(1)]. Therefore, we can choose a (topological) system of generators $\{\tau_\lambda\mid\lambda\in\Lambda\}$ of $G^T(\tilde{O}(K); K)$ $(\cong\mathbb{Z}_2^\Lambda)$ that is characterized by: For $\gamma\in\Lambda$, $\tau_\gamma(a_\gamma^{1/2^n})=\varepsilon_n a_\gamma^{1/2^n}$, for every $n\geqslant 1$, and $\tau_\gamma(a_\lambda^{1/2^n})=a_\lambda^{1/2^n}$, for every $n\geqslant 1$, and every $\lambda\neq\gamma$. Indeed, let $\gamma\in\Lambda$, and denote by E_γ the field obtained from $K^T=K^T(\tilde{O}(K); K)$ by adjoining all 2^nth roots of a_λ for all $n\geqslant 1$ and $\lambda\in\Lambda$, $\lambda\neq\gamma$. Using Corollary 3.9-(1) of [18] we get $E_\gamma^*=q(E_\gamma)\cup a_\gamma q(E_\gamma)$ and $G(E_\gamma)\cong\mathbb{Z}_2$ has a generator τ_γ such that $\tau_\gamma(a^{1/2^n})=\varepsilon_n a^{1/2^n}$, for every $n\geqslant 1$. The construction of E_γ, $\gamma\in\Lambda$, implies that $K^T \subseteq \bigcap E_\gamma = E$, $\gamma \in \Lambda$. It is easily seen that the image of $\{a_\lambda \mid \lambda \in \Lambda\}$ is a set linearly independent in $E^*/q(E)$. Since $E \mid K^T$ is a 2-extension we can conclude that $E = K^T$. Hence $\{\tau_\lambda \mid \lambda \in \Lambda\}$ is a system of generators of $G^T(\tilde{O}(K); K)$.

4.5. THEOREM. *Let K be a non-formally real C-field such that $(K^* : q(K)) > 2$ and there exists $r \geqslant 1$ for which $\varepsilon_r \notin K$. Then K fulfills the hypothesis of Theorem* 2.10 *and* $G(K) = G^T(\tilde{O}(K); K) \rtimes \mathbb{Z}_2$.

Furthermore, we can choose a generator σ for the $\mathbb{Z}_2$ component such that its action on the system of generators $\{\tau_\lambda \mid \lambda \in \Lambda\}$ of $G^T(\tilde{O}(K); K)$ (as constructed above) is described as follows:

(a) If $-1 \notin q(K)$ and $\varepsilon_n \in K(i)$ for every $n \geqslant 1$, then $\sigma \tau_\lambda \sigma^{-1} = \tau_\lambda^2$ for every $\lambda \in \Lambda$. In this case $G(K(i)) \cong G^T(\tilde{O}(K); K) \times \mathbb{Z}_2$ is the largest abelian normal subgroup of $G(K)$.

(b) If $-1 \notin q(K)$ and there exists n such that $\varepsilon_n \notin K(i)$, then $\sigma \tau_\lambda \sigma^{-1} = \tau_\lambda^{2^m - 1}$ for every $\lambda \in \Lambda$, where $m \geqslant 2$ satisfies the condition: $\varepsilon_{m+1} \in K(i)$ and $\varepsilon_{m+2} \notin K(i)$. Moreover, $G^T(\tilde{O}(K); K)$ is the largest abelian normal subgroup of $G(K)$.

(c) There exists $m \geqslant 2$ for which $\varepsilon_m \in K$ and $\varepsilon_{m+1} \notin K$. Then $G^T(\tilde{O}(K); K)$ is the largest abelian normal subgroup of $G(K)$ and $\sigma \tau_\lambda \sigma^{-1} = \tau_\lambda^{2^m + 1}$ for every $\lambda \in \Lambda$.

Proof. By Proposition 2.11, K fulfills the hypothesis of Theorem 2.10. Let $\mathscr{K}$ be the residue field of $O(K)$. Since K is a non-formally real field and $O(K)$ is 2-henselian, $\mathscr{K}$ is also a non-formally real field. For $r \geqslant 1$ such that $\varepsilon_r \notin K$ it follows that $\varepsilon_r \notin \mathscr{K}$, too. Hence $\mathscr{K}$ is not a quadratically closed field. Even more, $\mathscr{K}(2)$ is not a finite extension of $\mathscr{K}$, by [2, Satz 3]. We now determine $G(\mathscr{K})$. For the case (c) Theorem 2.10(b) yields $(O(K)^* q(K) : q(K)) \leqslant 2$. Hence $(\mathscr{K}^* : q(\mathscr{K})) \leqslant 2$. By the above observations $(\mathscr{K}^* : q(\mathscr{K})) = 2$ and so $G(\mathscr{K}) \cong \mathbb{Z}_2$. In the cases (a) and (b) K is not an exceptional field, so Theorem 2.10 yields $B(K) = O(K)^* q(K)$ and $B(\mathscr{K}) = \mathscr{K}^*$. Since $(B(K) : q(K)) = 2$ it follows from [1, Proposition 1.9-(2)] that $(\mathscr{K}^* : q(\mathscr{K})) = 2$, as well. Hence $G(\mathscr{K}) \cong \mathbb{Z}_2$ as in the case (c).

By [7, 20.10(b)], $G(K)/G^T(\tilde{O}(K); K) \cong G(\mathscr{K}) \cong \mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a free pro-2-group we get $G(K)$ as a semidirect product of $G^T(\tilde{O}(K); K)$ by $\mathbb{Z}_2$ as desired.

Let us now look for a suitable element $\sigma \in G(K)$ such that the subgroup $\langle \sigma \rangle$ yields the decomposition $G(K) = G^T(\tilde{O}(K); K) \rtimes \mathbb{Z}_2$. We also want σ which verifies the conditions (a)–(c) of the Theorem. Let $\{a_\lambda \mid \lambda \in \Lambda\} \subset K^*$ be chosen as we discussed above. Let E be the field obtained from K by adjoining 2^nth roots of a_λ, for all $n \geqslant 1$ and $\lambda \in \Lambda$, chosen as stated before

Lemma 3.3. Now observe that in cases (a) and (b) of the Theorem $\{a_\lambda \mid \lambda \in \Lambda\} \cup \{-1\}$ is an $\mathbb{F}_2$-basis of K^* modulo $q(K)$ while in case (c) $\{a_\lambda \mid \lambda \in \Lambda\} \cup \{\varepsilon_m\}$ is an $\mathbb{F}_2$-basis of K^* modulo $q(K)$. Hence in all three cases the unique quadratic extension of K inside $K^T(\tilde{O}(K); K)$ is not contained in E. So $K^T(\tilde{O}(K); K) \cap E = K$. Since $K^T(\tilde{O}(K) : K)E = K(2)$, $\mathbb{Z}_2 \cong G(K)/G^T(\tilde{O}(K); K) \cong G(E)$ by the Galois theory. Take now a generator σ of $G(E)$ and observe that for $\gamma \in \Lambda$, $\sigma\tau_\gamma\sigma^{-1}(a_\gamma^{1/2^n}) = \sigma(\varepsilon_n)\, a_\gamma^{1/2^n}$, for every $n \geqslant 1$, and $\sigma\tau_\gamma\sigma^{-1}(a_\lambda^{1/2^n}) = a_\lambda^{1/2^n}$, for every $n \geqslant 1$, and every $\lambda \neq \gamma$. Hence to get the action of σ on τ_λ, $\lambda \in \Lambda$, it suffices to determine $\sigma(\varepsilon_n)$ for every $n \geqslant 1$. In the case (a) $\sigma(\varepsilon_n) = \varepsilon_n^{-1}$ for every $n \geqslant 1$ since the restriction of σ to $K(i)$ is not trivial. For cases (b) and (c) observe first that $K^T(\tilde{O}(K); K)$ is the field obtained from K by adjoining all 2^nth roots of 1 for all $n \geqslant 1$. Moreover, $G(K^T(\tilde{O}(K); K); K)$ is a cyclic group. In case (b), $K(i)$ is the unique quadratic extension of K contained in $K^T(\tilde{O}(K); K)$. Thus $K(\sqrt{2}) \subseteq K(i)$ and $\varepsilon_3 \in K(i)$. Take $m \geqslant 2$ such that $\varepsilon_{m+1} \in K(i)$ and $\varepsilon_{m+2} \notin K(i)$. Now, arguing as in the proof of Theorem 3.4 (Case 2) we get $\sigma(\varepsilon_n) = \varepsilon_n^{-1}$ for every $1 \leqslant n \leqslant m$ and $\sigma(\varepsilon_{m+1}) = -\varepsilon_{m+1}^{-1}$. Thus σ can be chosen such that $\sigma(\varepsilon_n) = \varepsilon_n^{2^m - 1}$ for every $n \geqslant 1$. For the case (c) we can clearly choose σ such that $\sigma(\varepsilon_n) = \varepsilon_n^{2^m + 1}$ for every $n \geqslant 1$.

To complete the proof let U be an abelian normal subgroup of $G(K)$ and let F be its fixed field. If $r(U) > 1$, Theorem 4.1 implies $\varepsilon_n \in F$ for every $n \geqslant 1$. Hence F contains $K(i)$ in the case (a) and $K^T(\tilde{O}(K); K)$ in the cases (b) and (c). Thus $U \subseteq G(K(i))$ in the case (a) and $U \subseteq G^T(\tilde{O}(K); K)$ in the cases (b) and (c) as required.

Assume now $U \cong \mathbb{Z}_2$ and $C(U) = U$. By Theorem 3.4 the case (a) above cannot occur. Hence only cases (b) and (c) remain to be considered. We finish the proof using Corollary 3.5. Next, assume that there does not exist a normal subgroup U' of $G(K)$ such that $U \subseteq U'$, $U' \cong \mathbb{Z}_2$ and $C(U') = U'$. By Proposition 3.1 there exists a subgroup V of $G(K)$, such that $U \subset V$ and $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Let M be the fixed field of V. Thus $\varepsilon_n \in M \subset F$, by Theorem 4.1. Hence we complete the proof as in case of $r(U) > 1$. ∎

The examples (3), (4) and (5) presented in 4.11 show that all these possibilities may occur.

We shall now recollect the results about the existence of the largest normal abelian subgroup of $G(K)$ we have gotten so far. In the next theorem we shall also consider the formally real C-field and then complete our study.

4.6. THEOREM. *Let K be a field such that $(K^* : q(K)) > 2$.*

(a) *There exists the largest normal abelian subgroup $\mathfrak{U}$ of $G(K)$.*

Furthermore if $B(K) \neq \pm q(K)$, then $r(\mathfrak{U}) = r(K^*/B(K))$.

(b) $\mathfrak{U} = G^T(\tilde{O}(K); K)$, *unless K is a C-field such that $\varepsilon_n \in K(i)$ for every $n \geqslant 1$. This last case is classified according to*:

(b-1) *If $\varepsilon_n \in K$ for every $n \geqslant 1$, then $\mathfrak{U} = G(K)$ is described in Corollary* 4.2.

(b-2) *If K is a non-formally real field such that $-1 \notin q(K)$ and $\varepsilon_n \in K(i)$ for every $n \geqslant 1$, then $\mathfrak{U} = G(K(i)) = G^T(\tilde{O}(K); K) \times \mathbb{Z}_2$.*

(b-3) *If K is a formally real field, then $\mathfrak{U} = G(K(i))$ and either $\mathfrak{U} = G^T(\tilde{O}(K); K)$ if $\mathscr{K}_{O(K)}$ has just one ordering or $\mathfrak{U} = G^T(\tilde{O}(K); K) \times \mathbb{Z}_2$ if $\mathscr{K}_{O(K)}$ has two orderings.*

Proof. If $B(K) = K^*$, then $\mathfrak{U}$ is the trivial subgroup by Lemma 4.3. Assume now $B(K) \neq K^*$. If K is not a C-field the statements were proved in Theorem 4.4. If K is a non-formally real C-field such that $\varepsilon_r \notin K$ for some $r \geqslant 1$ the assertions were proved in Theorem 4.5. In the last case where K is a formally real C-field (a) follows from [3, Theorem 1, Chap. III, p. 86]. To prove (b-3) we apply Corollary 4.2 to $K(i)$. ∎

Now, as an application of the above results, we shall establish a relation between the subgroups of K^* containing $B(K)$ and the abelian normal subgroups U of $G(K)$. Our result generalizes Theorems B and C of [21] for arbitrary fields.

4.7. THEOREM. *Let K be a field such that $(K^* : q(K)) > 2$ and let α be any cardinal number. Let B_0 be either $B_0 = q(K) \cup \varepsilon_m q(K)$ if $B(K) = q(K)$ and $m \geqslant 2$ satisfies $\varepsilon_m \in K$ and $\varepsilon_{m+1} \notin K$ or $B_0 = B(K)$, otherwise.*

Then the following statements are equivalent:

(1) *There exists a subgroup H of K^* containing B_0 with $r(K^*/H) = \alpha$.*

(2) *There is a split exact sequence of pro-2-groups*

$$1 \to U \to G(K) \to V \to 1$$

with U abelian and $r(U) = \alpha$.

Proof. First we prove the equivalence for K a C-field. If $\varepsilon_n \in K$ for every $n \geqslant 1$, the result follows from Theorem 4.1. If $-1 \notin q(K)$ and K is a non-formally real field, then K is a non-exceptional field. Hence $B(K) = O(K)^*\, q(K)$ by Theorem 2.10(a) and $r(G^T(\tilde{O}(K); K)) = r(K^* : O(K)^*\, q(K))$ by Theorem 2.10(c). Finally, the equivalence follows from Theorem 4.5(a) and (b). If there exists $m \geqslant 2$ such that $\varepsilon_m \in K$ and $\varepsilon_{m+1} \notin K$ the equivalence follows from Theorem 4.5(c) and from the fact that $O(K)^*\, q(K) = q(K) \cup \varepsilon_m q(K)$. If K is a formally real field, then $q(K)$ is additively closed and K is a field hereditarily-pythagorean with respect to $K(2)$. By [3, Theorem 1, p. 86 and Lemma 2, p. 87] $G(K) = G(K(i)) \rtimes \langle \sigma \rangle$, where σ is an involution and $\sigma\tau\sigma^{-1}=\tau^{-1}$, for every $\tau\in G(K(i))$. By [12, Theorem 3.4, p. 202] $r(K(i)^*/q(K(i)))=r(K^*/B(K))$ and then the equivalence is clear.

We now take care of the non-C-field case. In this case $B(K)=O(K)^*\,q(K)$, by Theorem 2.10(a) and by Theorem 2.10(c), every subset $\{a_\lambda\mid\lambda\in\Lambda\}$ of K^* that is an $\mathbb{F}_2$-basis of K^* modulo $O(K)^*\,q(K)$ is also an $\mathbb{F}_2$-basis of $K^T(\tilde{O}(K);K)^*$ modulo $q(K^T(\tilde{O}(K);K))$.

(1)$\Rightarrow$(2). Let $\{a_\lambda\mid\lambda\in\Lambda\}$ be a set as above such that the images of the subset $\{a_\lambda\mid\lambda\in A\}$ is an $\mathbb{F}_2$-basis of K^*/H where A is a subset of Λ of cardinality α. Let E be the field obtained from $K^T(\tilde{O}(K);K)$ by adjoining all 2^nth roots of a_λ for all $n\geqslant 1$ and all $\lambda\in\Lambda$ and $\lambda\notin A$.

By an easy induction we can prove the following Lemma.

4.8. Lemma. *Let K be a field for which $-1\in q(K)$ and let $a_1,\dots,a_r$ be elements of K which are $\mathbb{F}_2$-independent module $q(K)$. Let $M=K(\{a_1^{1/2^n},\dots,a_r^{1/2^n}\})$, where $n\geqslant 1$ and $a_1^{1/2^n},\dots,a_r^{1/2^n}$ were chosen as it was stated before Lemma* 3.3. *Then $q(M)\cap K=\langle a_1q(K),\dots,a_rq(K)\rangle$.* ∎

We *claim* that $\{a_\lambda\mid\lambda\in A\}$ is an $\mathbb{F}_2$-basis of E^* module $q(E)$. In fact, let $\alpha_1,\dots,\alpha_r$ be distinct elements of A, $r\geqslant 1$, such that $a_{\alpha_1}a_{\alpha_2}\cdots a_{\alpha_r}=b^2$, where $b\in E$. Therefore, there exists $\lambda_1,\dots,\lambda_s\in\Lambda-A$, and $n\geqslant 1$ such that $b\in F$, where $F=K^T(\{a_{\lambda_1}^{1/2^n},\dots,\lambda_{\lambda_s}^{1/2^n}\})$ and $K^T=K^T(\tilde{O}(K);K)$. Thus $a_{\alpha_1}a_{\alpha_2}\cdots a_{\alpha_r}\in q(F)\cap K^T=\langle a_{\lambda_1}q(K^T),\dots,a_{\lambda_s}q(K^T)\rangle$, by the lemma above. This contradicts the choice of $\{a_\lambda\mid\lambda\in A\}$ since the sets $\{\alpha_1,\dots,\alpha_r\}$ and $\{\lambda_1,\dots,\lambda_S\}$ are disjoint. Hence $\{a_\lambda\mid\lambda\in A\}$ is $\mathbb{F}_2$-independent module $q(E)$.

Now, applying Lemma 3.4 of [18] to K^T we get that for every $x\in E$, there are $\beta_1,\dots,\beta_r\in\Lambda$, and $n\geqslant 1$ such that $x^{1/2}\in N$, where $N=K^T(\{a_{\beta_1}^{1/2^n},\dots,a_{\beta_r}^{1/2^n}\})$. Let $\{\alpha_1,\dots,\alpha_s\}=\{\beta_i\mid\beta_i\in A\}$ and $E'=EN$. Thus, $E'=E(\{a_{\alpha_1}^{1/2^n},\dots,a_{\alpha_s}^{1/2^n}\})$, and $x\in q(E')\cap E=\langle a_{\lambda_1}q(E),\dots,a_{\lambda_s}q(E)\rangle$, by Lemma 4.8. The *claim* is proved and so $r(G(E))=r(E^*/q(E))=\alpha$.

Now let $\rho\in G(K)$ and $\lambda\in\Lambda-A$. Then $\rho(a_\lambda^{1/2^n})=\varepsilon_n^j a_\lambda^{1/2^n}$ for some $1\leqslant j\leqslant 2^n-1$. So $\rho(E)=E$ and $E\mid K$ is a normal extension.

Let L be the field obtaining from K by adjoining 2^nth roots of a_λ, for every $n\geqslant 1$ and every $\lambda\in A$, chosen as it was stated before Lemma 3.2. Then $L\cap E=K$ and $LE=K(2)$, and if $U=G(E)$ we get the split exact sequence $1\to U\to G(K)\to V\to 1$, where $V\cong G(L)$.

(2)$\Rightarrow$(1). By Theorem 4.5 we have that $U\subseteq G^T(\tilde{O}(K);K)$. Thus $\alpha\leqslant|\Lambda|=r(K^*/q(B(K))$, so there exists a subgroup H of K^* such that $r(K^*/H)=\alpha$. ∎

At this point it is natural to ask for informations about the abelian subgroups of $G(K)$, that are not necessarily normal. In [22] Ware introduced a new invariant $a(K)$ for a field K, defined as follows:

4.9. Definition. $a(K)=\text{maximum}\{r(U)\mid U$ is an abelian subgroup of $G(K)\}$.

In his paper Ware studied this invariant and used valuation rings in order to give lower bounds of $a(K)$, [22, Corollary 2 of Theorem 1]. In the next theorem we improve this result.

Let us also recall that $G^Z(D; K)$ and $G^V(D; K)$, stand for the decomposition group and the ramification group of a valuation ring D of $K(2)$ over K, respectively. (See [7].)

4.10. THEOREM. *Let K be a field such that $(K^* : q(K)) > 2$ and let $\mathscr{A} = \{A \mid A \subseteq O(K)$ is a non-dyadic valuation ring of K with $\Gamma_A \neq 2\Gamma_A\}$. Then:*

(a) *If $\mathscr{A} \neq \varnothing$, then $\text{maximum}\{r(\Gamma_A/2\Gamma_A) \mid A \in \mathscr{A}\} \leqslant a(K) \leqslant \text{maximum}\{r(\Gamma_A/2\Gamma_A) + 1 \mid A \in \mathscr{A}\}$.*

(b) *If $\mathscr{A} = \varnothing$, then $a(K) = 1$.*

Proof. (a) If D is a valuation ring of $K(2)$ such that $D \cap K \in \mathscr{A}$, then $G^T(D; K)$ is an abelian subgroup of $G(K)$ of rank $r(\Gamma_A/2\Gamma_A)$. This proves the first inequality.

Now, let V be an abelian subgroup of $G(K)$, $r(V) \geqslant 2$ and E be its fixed field. By Corollary 4.2 we have either $V = G^T(\tilde{O}(E); E)$ or $V = G^T(\tilde{O}(E); E) \times \mathbb{Z}_2$. Thus $V \subseteq G^T(\tilde{O}(E); E) \times \mathbb{Z}_2 \subseteq G^T(\tilde{O}(E); K) \times \mathbb{Z}_2$. If $\tilde{O}(E) \cap K$ and $O(K)$ are not comparable valuation rings it follows from Proposition 2.4 that $G^T(\tilde{O}(E); K) = G^Z(\tilde{O}(E); K)$. By Theorem 2.14 it follows that $G^Z(\tilde{O}(E); K) \cap G^Z(\tilde{O}(K); K) = G^T(D; K)$, where D is the product of $\tilde{O}(E)$ and $\tilde{O}(K)$ (i.e., the smallest subring of $K(2)$ containing both $\tilde{O}(E)$ and $\tilde{O}(K)$). Since $G^Z(\tilde{O}(K); K) = G(K)$, then $G^Z(\tilde{O}(E); K) = G^T(D; K)$. As $\tilde{O}(K) \subseteq D$ it follows that $G^T(D; K) \subseteq G^T(\tilde{O}(K); K)$. Now, for $A = O(K)$ we have from the above considerations that $V \subseteq G^T(\tilde{O}(E); K) \times \mathbb{Z}_2 = G^Z(\tilde{O}(E); K) \times \mathbb{Z}_2 = G^T(D; K) \times \mathbb{Z}_2 \subseteq G^T(\tilde{O}(K); K) \times \mathbb{Z}_2$. So $r(V) \leqslant r(\Gamma_A/2\Gamma_A) + 1$.

Let us assume now that $\tilde{O}(E) \cap K$ and $O(K)$ are comparable. If $O(K) \subseteq \tilde{O}(E) \cap K$, we have $A = O(K)$ and if we argue as before we get $r(V) \leqslant r(\Gamma_A/2\Gamma_A) + 1$. Finally, if $\tilde{O}(E) \cap K \subseteq O(K)$, then we take $A = \tilde{O}(E) \cap K$. Since $r(V) \geqslant 2$ and $V \subseteq G^T(\tilde{O}(E); K) \times \mathbb{Z}_2$ it follows that Γ_A is not a 2-divisible group by [7, Theorem 20.19, p. 168]. So $A \in \mathscr{A}$. Recalling that $G^V(\tilde{O}(E); K)$ is trivial because $O(E)$ is a non-dyadic valuation ring we get again $r(V) \leqslant r(\Gamma_A/2\Gamma_A) + 1$, as required.

To prove (b) it suffices to show that if V is a non-trivial abelian subgroup of $G(K)$, then $r(V) = 1$. For such V let E be its fixed field. If $r(V) > 1$, we are going to prove that $\tilde{O}(E) \cap K \in \mathscr{A}$, contrary to $\mathscr{A} = \varnothing$. By Corollary 4.2, $G^T(\tilde{O}(E); E)$ is not trivial if $r(V) > 1$. Thus the value group of $\tilde{O}(E) \cap K^T(\tilde{O}(E); E)$ is not 2-divisible by [7, Theorem 20.12]. Since $K \subseteq K^T(\tilde{O}(E); E) \subset K(2)$, the same is true for $\tilde{O}(E) \cap K$. So $\tilde{O}(E) \cap K \in \mathscr{A}$ and the proof is finished. ∎

Next we construct some examples showing that these bounds are the best possible bounds. Our examples will also show that all the possibilities of the Theorems 4.2 and 4.5 may occur.

4.11. EXAMPLES. Let $K=k((X))^{\Gamma}$ be the field of generalized formal power series over a field k with respect to the lexicographic ordered group $\Gamma=\mathbb{Z}\times\mathbb{Z}$ and assume $c(k)\neq 2$. It is well known that the valuation ring $A=k[[X]]^{\Gamma}$ has value group Γ and residue class field k and is a henselian valuation ring.

(1) Let k be a quadratically closed field. Then, by [1, Proposition 1.5] $B(K)=q(K)$ and $\varepsilon_n\in K$ for every $n\geqslant 1$. Thus by Theorem 4.1 $G(K)$ is an abelian group. By construction $\Gamma_A\neq 2\Gamma_A$ and A is non-dyadic and 2-henselian (it is henselian already). Hence A is $q(K)$-compatible (see Remark 2.8). Since the residue class field $\mathscr{K}_A(=k)$ is quadratically closed, for every valuation ring A' of K such that $A'\subset A$, the value group of A' contains non-trivial 2-divisible convex subgroup. Hece $A=O(K)$ by Theorem 2.10. So $G(K)=G^Z(\tilde{O}(K);K)=G^T(\tilde{O}(K);K)\cong\mathbb{Z}_2\times\mathbb{Z}_2$.

(2) Let k be a field such that $c(k)\neq 2$, $\{\varepsilon_n\mid n\geqslant 1\}\subset k$, $G(k)\cong\mathbb{Z}_2$ and $K^Z(C;k)=k(2)$ for every non-trivial valuation ring C of $k(2)$ (for example: Let k be the field described in Remark 3.6(b-1)). From these properties we get $A=O(K)$ and for every valuation ring D of $K(2)$, $D\subseteq\tilde{O}(K)$, $G^T(D;K)=G^T(\tilde{O}(K);K)$. On the other hand, since $G(K)/G^T(\tilde{O}(K);K)\cong G(k)\cong\mathbb{Z}_2$, we have that $G(K)$ is metabelian. Hence K is a C-field by [19, Theorem 4.5]. Moreover, $\{\varepsilon_n\mid n\geqslant 1\}\subset K$. So $G(K)$ is an abelian group by Theorem 4.1. By (1) above $G^T(\tilde{O}(K);K)\cong\mathbb{Z}_2\times\mathbb{Z}_2$. Thus $G(K)=G^T(\tilde{O}(K);K)\times\mathbb{Z}_2\cong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

(3) Let F be an extension of $\mathbb{Q}$ such that F is non-real, $-1\notin q(F)$ and $\xi_n\in F$ for every $n\geqslant 1$ (for example: $F=\mathbb{Q}(\{\sqrt{-3}\}\cup\{\xi_n\mid n\geqslant 1\})$, where ξ_n, $n\geqslant 1$, were introduced in the proof of Lemma 3.3). Take an extension k of F such that $F\subseteq k\subset F(2)$ and k is maximal with respect to the exclusion of i. This means that every proper extension of k in $F(2)$ must contain i. Hence $G(k)$ is a cyclic group. Since $F\subseteq k$ and F is a non-formally real field $G(k)\cong\mathbb{Z}_2$. Now, we see that K is a C-field since $G(K)$ is metabelian (by the same arguments of the last example) and $\varepsilon_n\in K(i)$ for every $n\geqslant 1$. So, the condition (a) of Theorem 4.5 holds for K.

(4) As in the last example, let us take F to be an extension of $\mathbb{Q}$ which is non-real, $-1\notin q(F)$ and such that $\xi_m\notin F$ for some $m\geqslant 3$ and $\xi_n\in F$ for every $1\leqslant n\leqslant m$. Arguing as before we construct a field k that will provide K which fulfills the condition (b) of Theorem 4.5.

(5) Now we construct a field for which the condition (c) of Theorem 4.5 holds. As in example (3), take for F a field such that $\varepsilon_m\in F$

and $\varepsilon_{m+1} \notin F$ for some $m \geqslant 2$ and take k as a field containing F and maximal with respect to the exclusion of ε_{m+1}. The field K has the desired properties.

ACKNOWLEDGMENT

The authors are thankful to the referee for patiently reading this paper and making numerous helpful suggestions that clarify its final presentation.

REFERENCES

1. J. K. ARASON, R. ELMAN, AND B. JACOB, Rigid elements, valuations, and realization of Witt rings, *J. Algebra* **110** (1987), 449–467.
2. E. BECKER, Euklidische Körper und euklidische Hüllen von Körpern, *J. Reine Angew. Math.* **268–269** (1974), 41–52.
3. E. BECKER, "Hereditarily-Pythagorean Fields and Orderings of Higher Level," Monografias de Matematica 29, IMPA, Rio de Janeiro, 1978.
4. S. BREDIKHIN, YU. ERSHOV, AND V. KALNEI, Fields with two linear orderings, *Math. Zam.* **7** (1970), 525–536; (Also *Math. Notes* **7** (1970), 319–325).
5. L. BRÖCKER, Characterization of fans and hereditarily pythagorean fields, *Math. Z.* **151** (1976), 149–163.
6. A. DRESS, Metrische Ebenen über quadratisch perfekten Körper, *Arch. Math.* **92** (1966), 19–29.
7. O. ENDLER, "Valuation Theory," Springer Verlag, Berlin/Heidelberg/New York, 1972.
8. O. ENDLER, On Henselization of valued fields, *Bol. Soc. Brasil. Mat.* **4** (1973), 97–109.
9. O. ENDLER AND A. J. ENGLER, Fields with henselian valuation rings, *Math. Z.* **152** (1977), 191–193.
10. A. J. ENGLER, Fields with two incomparable henselian valuation rings, *Manuscripta Math.* **23** (1978), 373–385.
11. A. J. ENGLER AND T. M. VISWANATHAN, Digging holes in algebraic closures a la Artin I, *Math. Ann.* **265** (1983), 263–271.
12. T. Y. LAM, "The Algebraic Theory of Quadratic Forms," Benjamin, New York, 1973.
13. T. Y. LAM, "Orderings, Valuations and Quadratic Forms," Conference Board of the Mathematical Sciences, Number 52, Amer. Math. Soc., Providence, RI, 1983.
14. A. LUBOTZKY, Combinatorial group theory for pro-p groups, *J. Pure Appl. Algebra* **25** (1982), 311–325.
15. L. RIBES, "Introduction of Profinite Groups and Galois Cohomology," Queen's Papers in Pure and Applied Mathematics, Vol. 24, Queen's University, Kingston, 1970.
16. J-P. SERRE, "Cours d'Arithmétiques," Presses Universitaires de France, Paris, 1970.
17. L. P. D. VAN DEN DRIES, "Model Theory of Fields," Thesis, University of Utrecht, 1979.
18. R. WARE, When are Witt rings group rings? II, *Pacific J. Math.* **76** (1978), 541–564.
19. R. WARE, Quadratic forms and profinite-2-groups, *J. Algebra* **58** (1979), 227–237.
20. R. WARE, Valuation rings and rigid elements in fields, *Canad. J. Math.* **33** (1981), 1338–1355.
21. R. WARE, Quadratic forms and pro-2-groups. III. Rigid elements and semidirect products, *Comm. Algebra* **13** (1985), 1713–1736.
22. R. WARE, Stability in Witt rings and abelian subgroups of pro-2-groups, *Rocky Mountain J. Math.* **19** (1989), 985–995.